

APOGEE Communications

Rapport de Veille Technologique Sécurité N°65

Décembre 2003

Les informations fournies dans ce document ont été collectées et compilées à partir de sources d'origines diverses et publiquement accessibles: mailing-lists, newsgroups, sites Web, ...

Ces informations sont fournies pour ce qu'elles valent sans garantie d'aucune sorte vis à vis de l'exactitude, de la précision ou de la qualité de l'information. Les URL associées à certains thèmes sont validées à la date de la rédaction du document.

Les symboles d'avertissement suivants seront éventuellement utilisés:

Site dont la consultation est susceptible de générer directement ou indirectement, une attaque sur l'équipement de consultation, voire de faire encourir un risque sur le système d'information associé.

Site susceptible d'héberger des informations ou des programmes dont l'utilisation est répréhensible au titre de la Loi Française.

Aucune garantie ne peut être apportée sur l'innocuité de ces sites, et en particulier, sur la qualité des applets et autres ressources présentées au navigateur **WEB**.

**La diffusion de ce document est restreinte aux
clients des services
VTS-RAPPORT et VTS-ENTREPRISE**

Les marques et les produits cités dans ce rapport sont la propriété des dépositaires respectifs.

Au sommaire de ce rapport ...

PRODUITS ET TECHNOLOGIES	5
LES PRODUITS	5
INTERNET EXPLORER	5
PIVX - QWIK-FIX	5
OUTILS	6
KNOPPIX - STD VS PHLAK	6
INFORMATIONS ET LÉGISLATION	9
LES INFORMATIONS	9
SÉCURISATION	9
WINDOWS – IDENTIFICATION DES PROCESSUS	9
SQLSERVER – LE ROLE 'PUBLIC'	9
CERT – AVANT DE CONNECTER UN NOUVEAU SYSTÈME SUR INTERNET	10
NSA - CATALOGUE DES GUIDES DE SÉCURITÉ	11
CRYPTOGRAPHIE	12
CHALLENGE RSA-576	12
LA LÉGISLATION	13
SÉCURITÉ	13
EU - CRÉATION DE L'AGENCE EUROPÉENNE CHARGÉE DE LA SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION	13
LOGICIELS LIBRES	14
LES SERVICES DE BASE	14
LES OUTILS	14
NORMES ET STANDARDS	16
LES PUBLICATIONS DE L'IETF	16
LES RFC	16
LES DRAFTS	16
NOS COMMENTAIRES	21
LES RFC	21
RFC 3299/3499/3599	21
LES DRAFTS	22
DRAFT-IETF-PKIX-LOGOTYPES	22
ALERTES ET ATTAQUES	23
ALERTES	23
GUIDE DE LECTURE	23
FORMAT DE LA PRÉSENTATION	24
SYNTHÈSE MENSUELLE	24
ALERTES DÉTAILLÉES	25
AVIS OFFICIELS	25
APPLE	25
BIND	25
CA	25
CISCO	25
CVS	26
ETHERREAL	26
GNU PG	26
HP	26
IBM	26
KERIO	27
LINUX	27
LINUX SuSE	27
MACROMEDIA	27
MODPYTHON	27
NOVELL	27
OPERA	28
SOAP	28
SUN	28
ALERTES NON CONFIRMÉES	29
APPLE	29
APPLIED WATCH	30
ARC	30
CYBERGUARD	30

DAMEWARE	30
FREERADIUS	30
GNU	30
IBM	30
IKE	30
IPSWITCH	31
L-SOFT	31
LFTP	31
LINKSYS	31
MACROMEDIA	31
MICROSOFT	31
NETGEAR	32
OPENCA	32
PHP	32
SQUIRRELMAIL	32
SYBASE	32
WEBSense	32
XEROX	32
YAHOO!	33
AUTRES INFORMATIONS	33
REPRISES D'AVIS ET CORRECTIFS	33
APPLE	33
CERT	33
CIAC	33
FREEBSD	34
HP	34
HP/COMPAQ	35
ISC	36
IBM	36
LINUX DEBIAN	36
LINUX MANDRAKE	36
LINUX REDHAT	36
MICROSOFT	36
MOZILLA	37
NOVELL	37
NetBSD	37
ORACLE	37
SCO	37
SGI	37
SUN	38
TARANTELLA	39
CODES D'EXPLOITATION	39
DAMEWARE	39
BULLETINS ET NOTES	39
ATTAKUES	39
MICROSOFT	39
ATTAKUES	40
OUTILS	40
FTWALL - KAZAA	40
DÉTÉSCAN / ANAPIRATE	41
TECHNIQUES	45
MALWARE	45
DIGRESSIONS AUTOUR DE L'ENCODAGE ASN.1	46

Le mot de la rédaction ...

Après la technologie '**Wifi**', c'est la technologie '**Bluetooth**' qui pourrait bien faire la Une des articles consacrés à la sécurité. Si les équipements de première génération ne posaient pas de véritable problème de sécurité étant donnée leur portée réduite, la nouvelle génération qui devrait arriver prochainement en masse sur le marché pourrait conduire à devoir modifier la position des spécialistes de la sécurité.

Avec une portée étendue à 100 mètres et une intégration de fait dans la majorité des dispositifs de communication récents, cette technologie offre une nouvelle possibilité d'accès aux données personnelles ou professionnelles stockées dans ces dispositifs. Les règles de sécurité applicables aux réseaux '**WiFi**' vont devoir être adaptées pour tenir compte des caractéristiques propres à la technologie '**Bluetooth**' offrant un véritable bus de communication sans fil.

Nous recommandons la lecture du communiqué de presse publié à ce sujet par la société '@Stake' bien connue de nos lecteurs.

http://www.atstake.com/events_news/press_releases/template.html?europe/121603

Dans un tout autre registre, nous regrettons le silence entourant le futur des défis proposés régulièrement depuis maintenant 3 ans par l'équipe du projet **HoneyNet**. On ne peut qu'espérer qu'il ne s'agisse que d'un arrêt temporaire et qu'une nouvelle série de défis verra le jour l'année prochaine.

Enfin, l'**IETF** a annoncé que le moteur de filtrage '**SpamAssassin**' serait activé mi-décembre sur son système de messagerie afin de prévenir toute tentative de détournement de celui-ci.

This is to inform you that we are planning to turn on SpamAssassin on all IETF mail on Monday 12/15 at 3PM Eastern Time. The only thing SpamAssassin will be doing at this time is adding headers to messages indicating whether or not it believes a message is or is not spam. We will reserve the ability to do filtering based on these headers until a later time after more analysis is performed.

On ne peut qu'espérer que cette démarche soit suivie par les autres grandes organisations pour lesquelles le système de messagerie représente un moyen privilégié de communication notamment par le biais des listes de diffusions.



Nous terminerons notre propos en souhaitant une bonne Année 2004
à tous nos lecteurs

L'équipe de Veille Technologique

PRODUITS ET TECHNOLOGIES

LES PRODUITS

INTERNET EXPLORER

PIVX - QWIK-FIX

Description

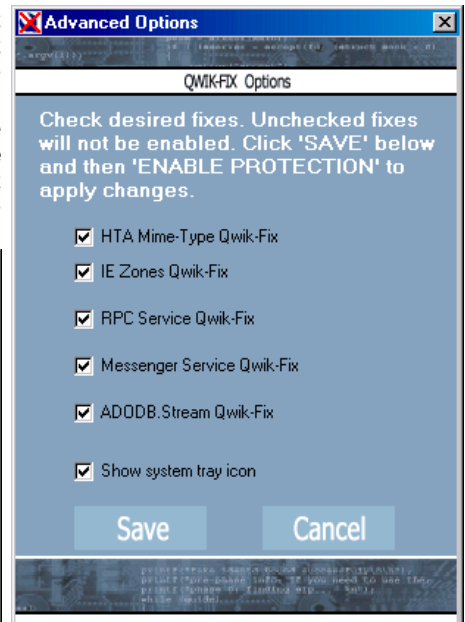
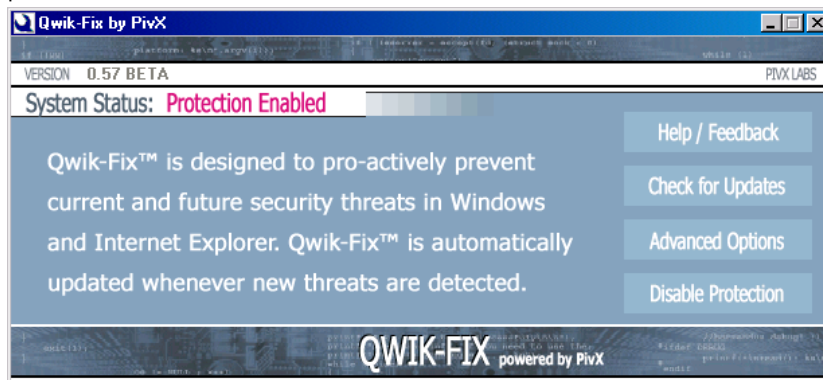
Qwik-Fix Présenté comme un produit miracle permettant de prévenir des atteintes susceptibles d'être perpétrées via des vulnérabilités n'ayant pas encore fait l'objet de correctifs, 'Qwik-Fix' est disponible gratuitement sur le site de la société de 'Thor Larholm' bien connu des lecteurs de la liste 'BugTraq'.

'Qwik-Fix' est ainsi annoncé corriger les problèmes de gestion des zones de sécurité en environnement Internet Explorer, les problèmes 'RPC/DCOM', les vulnérabilités liées au service 'Messenger', la faille présente dans la gestion des flux ADO et pour finir les vulnérabilités liées à la gestion du type Mime 'HTA' !

Cette annonce est presque trop belle pour être vraie d'autant qu'aucune information n'est fournie sur la technologie sous-jacente par ailleurs annoncée pouvoir parer à toutes les vulnérabilités connues dans Windows ou Internet Explorer, et ce dans l'attente de la fourniture du correctif mensuel promis par Microsoft.

Nous avons décidé de tester ce produit en considérant qu'il serait cependant difficile d'évaluer son efficacité réelle, aucune série de tests n'étant disponible dans ce contexte contrairement à ce qui se pratique dans le domaine de la protection anti-virale.

L'installation de 'Qwik-Fix' est aisée et sans aucune surprise. Une icône présente dans la barre des tâches permet d'accéder à la fenêtre de configuration permettant de désactiver la protection pour éventuellement modifier la liste des protections proposées ou encore mettre à jour le produit.



Le fonctionnement de 'Qwik-Fix' est totalement transparent et il ne nous a pas été possible d'obtenir la moindre fenêtre de notification malgré nos tentatives d'attaque sur la machine protégée par cette application.

L'analyse des fichiers livrés avec l'application permet heureusement de comprendre la technique employée pour renforcer la gestion des zones de sécurité sous Internet Explorer.

La lecture du fichier 'ac' révèle en effet que celui-ci contient la liste des identifiants – ou **CLSID** - de 82 objets **Active / X** qui seront inscrits sous la clef de registre '**HKLM\Software\Policies\Microsoft\ Windows\Current Version\AllowedControls**'.

L'article '**Q182569**' de la base de connaissance précise que cette clef permet de spécifier les seuls objets dont l'exécution sera implicitement autorisée.

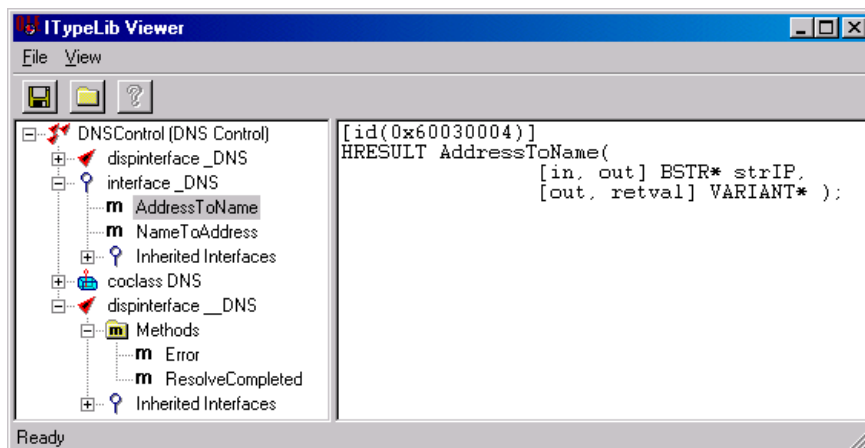
Son association avec la clef '**Internet Settings**' et diverses clefs dérivées permet ainsi de restreindre les fonctionnalités et autorisations d'exécution en environnement Internet Explorer V6 au strict minimum requis. Nous laissons le soin au lecteur intéressé de rechercher le nom des objets ainsi autorisés.

L'un des objets référencés apparaît être le control nommé 'DNSControl'. Celui-ci est implémenté dans la librairie 'DNS.ocx' livrée avec le paquetage 'Qwik-Fix'.

Les différentes méthodes exposées par cet objet montrent qu'il implémente les fonctions classiques de résolution d'un nom à partir de l'adresse IP et vice-versa.

Le rôle exact de cet objet dans le mécanisme de protection reste cependant impossible à déterminer.

Plus largement, aucun élément ne permet de déterminer si 'Qwik-Fix' joue un rôle de protection dynamique et si oui, comment.



Une rapide étude de l'exécutable 'QwikFix.exe' montre, après décompression, que l'application a été écrite en Visual Basic et révèle certaines des techniques utilisées pour assurer les autres fonctions de protection :

- Modification de la clef référençant le type MIME 'application/hta' en 'application/hta1928' afin de rendre inopérant les traitements associés aux documents utilisant ce type de contenu, et donc d'éliminer les risques d'attaque tirant parti de la vulnérabilité associée,
- Modification de la clef autorisant l'activation des services 'DCOM' sur les interfaces réseaux,
- Désactivation du service 'Messenger' en inhibant le démarrage automatique et en arrêtant le service actif,
- ...

On remarquera aussi la présence dans le code de l'adresse IP '64.186.255.98' qui se révèle être celle du site 'qwikfix.pivx.com' hébergeant les mises à jour du produit.

Notre première impression est que 'Qwik-Fix' n'apporte rien qui ne puisse être effectué par le biais d'un script de configuration voire même par un fichier de configuration 'GPO' mais peut être n'avons nous pas découvert toutes les subtilités du produit. L'utilisateur n'encourt cependant pas grand risque à installer cet utilitaire et à faire sien le pari de Pascal. Il devra pourtant prendre garde au fait que la protection statique apportée par 'Qwik-Fix' n'est pas permanente, les paramètres de la base de registre étant repositionnés à leur valeur originale si l'on quitte l'application.

• Complément d'information

<http://www.pivx.com/qwikfix/faq.html>

<http://support.microsoft.com/support/kb/articles/Q182/5/69.ASP&NoWebContent=1>

- Foire aux questions

- Article de la base de connaissance

OUTILS

KNOPPIX - STD VS PHLAK

• Description

KNOPPIX.net Parmi les distributions 'LINUX' autonomes – dites 'Live CD' – la distribution Knoppix basée sur l'environnement DEBIAN semble rapporter un succès considérable.

Sont ainsi actuellement répertoriées quelques 11 variations francisées de cette distribution dont notamment la version orientée sécurité dite 'Knoppix-MIB' du nom de son concepteur Michel Bouissou (Rapport N°58 – Mai 2003).

Deux autres versions spécialisées dans le domaine de l'audit et des tests de sécurité ont vu le jour dernièrement et quasiment simultanément :

- la version Knoppix STD diffusée en octobre dernier,
- la version Knoppix PHLAK elle aussi diffusée pour la première fois en octobre dernier mais ayant déjà fait l'objet d'une mise à jour.

Une liste, non exhaustive, des principales applications et outils intégrés dans ces deux distributions est proposée ci-dessous. Nous y avons rajouté à titre indicatif la distribution 'PenguinSleuth' toujours basée sur Knoppix mais réalisée à l'attention de ses homologues par Ernest Baca, un spécialiste américain de l'investigation informatique.

	Knoppix STD	Knoppix PHLAK	Penguin Sleuth
Version courante	V0.1b	V0.2	V1.1
Utilisation	Audit, Test de pénétration	Audit, Test de pénétration	Forensic
Organisation	Arborescence Thématique	Arborescence Unix	Arborescence Dédié
Utilitaires LINUX			
Audit			
Amap	2.5	X	
Chkrootkit	0.4	X	X
dnswalk		X	
flawfinder		X	
hammerhead		X	
hping2	X	x	X
idswakeup		X	

Nasl	X	x	
nbtscan		X	X
Nessus	2.0.4	x	X
nikto		X	X
Nmap	3.10	x	
p0f			
pncan		X	
Rpcinfo	X		
Snort	X		X
scanssh		X	X
ssldump		X	
xprobe			X
Whisker	2.1		
Winscan	X		
Authentification			
freeRadius	0.8.1		
PAM config	X		
Cassage de mots de passe			
Cracklib2		X	
John the ripper	1.6	X	X
Chiffrement			
CryptCat	X	X	
GPG	1.2.1	X	X
OpenSSL	0.9.7a	X	
SSLWrap	X		
sTunnel	X		X
Firewall			
Freeswan		X	
Gtk-IpTables	X		
ipchains		X	
IpTables	1.27a		
ShoreWall	1.4		
Forensic			
AutoPsy	1.71	X	X
dcfldd			X
Fenris	0.7	X	
foremost			X
MacRobber	1.0		X
Outils basics: dd, lsof, strings, grep	X	X	X
Secure_Delete	X		
SleuthKit	1.61	X	X
Wipe	X	X	X
Journalisation			
Aide	0.9	X	
Argus		X	
Snort	1.8.7-4		
Swatch	3.0.1		
SysLogd	X		
Pot de Miel			
Honeyd	0.5-2		X
Labrea	2.3-2		
Réseau			
Arping	X	X	
Arpd		X	
Arptool	X		
Arpwatch	X	X	X
Cheops	0.61-4	X	
dig			X
dsniff	2.4		X
ethereal	0.9.5	X	X
EtherRape	0.8.2-3	X	X
ettercap	0.6.a	X	X
echoping		X	
farpd		X	
fping		X	X
fragroute		X	X
icmpinfo		X	
icmppush		X	
Ip-sorcerer	X		
Iptraf	X	X	
LinNeighborhood	X		
Macchanger	X	X	
Mtr	X		
nemesis	1.4.beta 1	X	X
netsed	X	X	
ngrep	X	X	X
Ntop	2.1.0	X	

nstreams		X	
paketto	1.10	X	
rarpd		X	
Samba	2.2.3.a		
tcpdump	3.6	X	X
tcpflow		X	
tcpreplay	1.4.0	X	X
Service			
Apache	1.3.27		
Bind9	X		
Httpunnel	X	X	
Iacd	X		
Netcat	X		X
net-snmp	X		
smail	3.2		
sshd	X		
stunnel		X	
tftpd	X		
vnc	X		
Xinetd	X		
WiFi			
AirSnort	X	X	X
WarDrive	X		
KisMet	2.6.2	X	X
MacChanger	X		
Utilitaires Windows			
achilles		X	
AinTx		X	
Brutus		X	
THC-CuPass		X	
ispy		X	
nbtDump		X	
photorec		X	
md5deep		X	
pdd		X	

Cette liste comparative met bien en évidence les deux problèmes endémiques à toutes les distributions autonomes, à savoir :

- une sélection 'anarchique' des outils et applications embarquées, en notant toutefois que la distribution '**PHLAK**' intègre nombre de paquets directement issus de l'environnement natif '**Debian**'. Ce phénomène est directement lié au concept même du '**LiveCD**' véritable reflet de la pensée et de l'organisation de son concepteur. On regrettera la prolifération actuellement constatée de distributions n'ayant pas grand intérêt quand l'énergie ainsi dépensée pourrait être mieux employée à la création d'un système de génération automatique de distributions 'Live'.
- l'utilisation de versions de logiciels notoirement obsolètes – voire dangereux du point de vue de la sécurité - intégrés à des distributions pourtant récentes. Ce problème vient conforter notre position précédente et milite en faveur de la création d'outils facilitant la régénération automatique d'une distribution à partir d'un modèle type.

Les distributions **Knoppix STD** et **Knoppix PHLAK** viennent concurrencer les remarquables paquets '**F.I.R.E**' (ex **Biatchux**) et '**Trinux**' (Rapport N°43 – Février 2002).

A ce jour, et de notre point de vue, notre choix préférentiel se porte toujours sur la distribution '**F.I.R.E**', complète, mature et intégrant outre les paquets **LINUX**, divers utilitaires destinés à être activés en environnement **Windows** et **Solaris**. Bien moins mature, la distribution '**PHLAK**' n'en présente pas moins l'intérêt de s'appuyer sur la distribution '**Knoppix**' remarquablement stable et complète notamment en terme de support du matériel hôte.

Au risque de se voir reprocher de vouloir créer une n-ième distribution, nous concluons en suggérant à l'auditeur ou au consultant de sécurité de tester les distributions '**F.I.R.E**' et '**Knoppix PHLAK**' pour retenir celle la plus adaptée en complétant celle-ci avec les utilitaires requis mais absents.

• Complément d'information

<http://knoppix-std.org/>

<http://www.phlak.org/>

<http://knoppixfr.tuxfamily.org/index.php?page=download#knoppixmib>

<http://www.knoppix.net>

<http://www.linux-forensics.com/downloads.html>

<http://www.distrowatch.com/dwres.php?resource=cd>

- Distribution **Knoppix-STD**

- Distribution **Knoppix-PHLAK**

- Distribution **Knoppix-MIB**

- Distribution originale de **Knoppix**

- Distribution PenguinSleuth

- Liste des distributions 'LiveCD'

INFORMATIONS ET LEGISLATION

LES INFORMATIONS

SÉCURISATION

WINDOWS – IDENTIFICATION DES PROCESSUS

•Description



Le site '**AnswersThatWork**' propose une intéressante liste des processus s'exécutant en tâche de fond en environnement Windows.

L'utilisateur mais surtout l'exploitant pourront ainsi identifier explicitement les applications actives autrement que par un nom abscons tel que '**lsass.exe**' ou encore '**msimm.exe**' pour ne citer que deux exemples classiques.

Cette liste est présentée sous la forme d'un tableau de trois colonnes dont la première référence le nom du processus, la seconde indique le nom de l'application ayant activé ce processus et la dernière propose un commentaire apportant diverses précisions techniques.

Un index alphabétique permet d'accélérer l'accès aux informations contenues dans ce tableau dont un extrait est proposé ci-contre pour exemple.

Nous avons particulièrement apprécié en maintes occasions la pertinence des éléments fournis en regrettant cependant de ne pas disposer d'une interface de recherche plus évoluée.

Acrotray	AcroTray.exe (Adobe)	Adobe Acrobat Assistant. This background task is installed when you install the full version of Adobe Acrobat. It comes into action when you create PDF files from non Adobe applications through the "Watched Folders" feature of Acrobat Distiller. Recommendation : Usually harmless. Only disable with Startup Manager if you specifically experience problems with it.
Activation	Activation.exe (Microsoft)	Microsoft's Activation module for their Windows XP and Microsoft Office XP/2002 products. Recommendation : Leave alone. We are not yet sure as to how exactly ACTIVATION.EXE works; however, given the problems one can run into with inactivated Windows XP / Office XP / Office 2002 products at the best of times, we do not recommend doing anything with this background task.
Addrbook	Addrbook.exe	Novell GroupWise Address Book. This task appears when you first use the GroupWise

•Complément d'information

http://www.answersthatwork.com/Tasklist_pages/tasklist.htm

SQLSERVER – LE RÔLE 'PUBLIC'

•Description

Le document intitulé '**SQL Server 2000 : Permissions on System Tables granted to logins due to the public role**' a été publié sur le site du **SANS Institute** dans le cadre de la certification **GIAC** délivrée par ce même organisme.

Ce document est particulièrement intéressant car il aborde un sujet peu documenté, celui des privilèges accordés à certains rôles prédéfinis dans les systèmes de base de données, dans le cas présent, le système '**SQLServer**'.

A travers une analyse méthodique et rigoureuse, l'auteur met en lumière les problèmes posés par le rôle '**Public**' normalement attaché à tout nouvel utilisateur, et notamment, le non respect du principe du moindre privilège par les concepteurs de ce système de base de données. Ainsi, de nombreuses tables systèmes et procédures stockées dont l'utilisation n'est pas requise pour l'utilisateur lambda sont pourtant rendues accessibles par ce rôle.

Brian Kelley, l'auteur de ce document, démontre que ce problème de sécurité est aggravé par l'existence d'un utilisateur spécial, dit '**guest**', attaché à chaque base de données. Cet utilisateur peut être activé pour offrir un accès restreint aux comptes d'accès – dit 'login' – non associés à un utilisateur déclaré sur la base de données. On devine aisément les conséquences qui découlent du fait que le rôle '**Public**' est automatiquement attaché à l'utilisateur '**guest**' et que ce dernier a la visibilité des bases systèmes **Master** et **Msdb** ...

Deux questions se posent alors:

- quelles sont les tables impactées par l'autorisation d'accès liée au rôle 'Public',
- quels sont les risques encourus à révoquer l'accès du rôle 'Public' sur ces tables.

S'il est relativement aisé de répondre à la première question en utilisant les fonctionnalités offertes par le langage SQL, la seconde question requiert d'employer une approche moins rigoureuse consistant à révoquer les accès 'Public' table par table jusqu'à constater un dysfonctionnement de l'application sélectionnée pour le test. Autant dire que cette approche ne peut garantir que le résultat sera applicable à tous les contextes.

Fort heureusement, bien que peu d'information ait été publiée par la société **Microsoft** à ce propos, les documents

diffusés à l'occasion du dernier défi '**OpenHack**' viennent à notre secours. Publiquement relevé par les sociétés Microsoft et Oracle, ce défi dont la dernière édition a eu lieu en novembre 2002 avait pour objectif d'attaquer une architecture **WEB** dont la configuration avait été préalablement optimisée par chaque participant. Les résultats ont démontré qu'un excellent niveau de sécurité pouvait être atteint moyennant l'utilisation d'une configuration particulièrement soignée.

Ainsi, et dans le cas de la base **SQLServer** utilisée dans le cadre de ce défi, les accès du rôle 'Public' avaient été révoqués sur toutes les tables à l'exception d'une table et d'une procédure stockée. Cette configuration on ne peut plus restrictive n'est hélas pas applicable dans la majorité des environnements et notamment ceux utilisant un client **Microsoft Access** ou encore des connexions **DSN** sur la base de données. On pourra cependant s'inspirer de la démarche suggérée par Microsoft et des résultats de l'étude menée par **Brian Kelley**.

Le lecteur trouvera dans cette étude une liste non exhaustive des procédures stockées rendues exécutables via le rôle 'Public' et des tables systèmes avec, pour ces dernières, une indication du niveau de risque: '**Secure**' (aucun risque d'exposition d'information), '**Insecure**' (risque avéré de fuite d'information sensible) et '**Not sensitive**' (fuite possible d'informations publiques).

Un tableau récapitulatif est proposé ci-dessous, le lecteur se reportera avec intérêt aux commentaires présentés dans le rapport d'étude pour mesurer le degré d'exposition des données contenues dans les tables.

Contexte	Nom de la table	Niveau de risque
Master Database	sysconfigures	Insecure
	syscurconfigs	Insecure
	sysdatabases	Insecure
	sysdevices	Insecure
	syslockinfo	Insecure
	syslocks	Insecure
	sysmessages	Insecure
	sysservers	Insecure
	sysaltfiles	Secure
	syscacheobjects	Secure
	syscursorscolumns	Secure
	syscursorrefs	Secure
	syscursortables	Secure
	sysperfinfo	Secure
	sysprocesses	Secure
	sysxlogins	Secure
	syscharsets	Not sensitive
	syslanguages	Not sensitive

Contexte	Nom de la table	Niveau de risque
User Databases	syscolumns	Insecure
	syscomments	Insecure
	sysdepends	Insecure
	sysfilegroups	Insecure
	sysfiles	Insecure
	sysforeignkeys	Insecure
	sysfulltextcatalogs	Insecure
	sysindexes	Insecure
	sysindexkeys	Insecure
	sysmembers	Insecure
	sysobjects	Insecure
	syspermissions	Insecure
	sysprotects	Insecure
	sysreferences	Insecure
	systypes	Insecure
	sysusers	Insecure
	sysfiles1	Secure
	sysfulltextnotify	Secure
	sysproperties	Secure

Contexte	Nom de la table	Niveau de risque
MSDB	Backup	Insecure
	LogMarkHistory	Insecure
	MSWebTasks	Insecure
	Restore	Insecure
	RTbl	Not sensitive
	syscategories	Not sensitive

• Complément d'information

<http://www.sans.org/rr/papers/index.php?id=1273>

<http://www.eweek.com/article2/0,4149,743002,00.asp>

- Dossier

- OpenHack 4

CERT – AVANT DE CONNECTER UN NOUVEAU SYSTEME SUR INTERNET

• Description



Le **CERT-CC** publie régulièrement une série de notes techniques – ou '**tech-tips**' – simples et concises traitant de manière approfondie d'un sujet ayant trait à la sécurité. Ainsi, et à ce jour, quelques 39 notes techniques ont été publiées dans l'une des huit catégories suivantes:

- **Sécurisation des SI:** 8 documents
- **Réponse aux incidents:** 8 documents
- **Sécurité des sites WEB:** 4 documents
- **Abus de la messagerie:** 2 documents
- **Comprendre les attaques:** 5 documents
- **Connaissance technique:** 2 documents
- **Ordinateurs personnels:** 2 documents
- **Autres sujets:** 8 documents

Diffusée mi-décembre, la note intitulée '**Before You Connect a New Computer to the Internet**' aborde un thème d'autant plus pertinent qu'il intéresse l'utilisateur aussi bien dans le cadre professionnel que dans le cadre privé. Qui de nos jours n'a pas eu à raccorder son ordinateur personnel sur **Internet**, ordinateur par ailleurs susceptible d'être employé pour travailler sur des dossiers professionnels en retard et pour lequel la sécurité reste un pré-requis ?

Si a priori, l'installation d'un ordinateur et son raccordement sur Internet peut sembler une opération bénigne, l'expérience montre qu'il n'en est rien notamment en ce qui concerne les opérations de mise à jour du système d'exploitation et des applications associées.

Nombreux sont les exemples de systèmes ayant été compromis durant la phase de mise à jour effectuée via le réseau. La courte fenêtre de quelques minutes durant laquelle le système tout juste installé est encore vulnérable suffit pour que celui-ci soit sondé, identifié puis immédiatement compromis.

La parade la plus efficace consiste à respecter une procédure d'installation prenant en compte les risques associés à chacune des étapes. Ainsi, et dans le cas des exemples précédemment cités, la désactivation des services sensibles ou encore la mise en place, préalable à la mise à jour via Internet, d'un dispositif de protection personnel aurait permis d'éviter la compromission du système.

Dans sa note technique, le **CERT-CC** propose un mode opératoire en quatre phases permettant d'assurer le raccordement d'un système **Windows XP** ou **MacIntosh OS X** en encourant un minimum de risque:

- 1- Dans la mesure du possible positionner le système derrière un pare-feu réseau,
- 2- Activer le pare-feu logiciel généralement livré avec le système d'exploitation, service 'ICF' en environnement Windows ou 'Firewall' en environnement MacOS X,
- 3- Désactiver tous les services non absolument essentiels à l'opération de mise à jour et notamment les services de partage de fichiers et d'imprimantes. Ces services pourront être réactivés une fois la mise à jour effectuée,
- 4- Enfin, connecter le système au réseau et télécharger les mises à jour depuis un site réputé de confiance.

• Complément d'information

http://www.cert.org/tech_tips/before_you_plug_in.html

- Recommandations du **CERT**

NSA - CATALOGUE DES GUIDES DE SECURITE

• Description



La parution d'une nouvelle version du 'Guide to the Secure Configuration and Administration of Microsoft Exchange 2000' (Rapport N°47 – Juin 2002) nous amène à publier la mise à jour de notre catalogue qui liste ces documents en mettant en évidence le thème de rattachement, le titre, le numéro de révision et la date de publication.

Les codes suivants sont utilisés :

- | | | | |
|---|---|---|-------------------------------|
| I | Document d'information et/ou de synthèse | ✓ | Document récemment mis à jour |
| G | Guide de mise en œuvre et/ou manuel d'utilisation | ✍ | Document nouvellement publié |
| R | Recommandations et principes élémentaires | | |
| P | Procédures et mise en application | | |

Windows XP

Système

G	Guide to Securing Microsoft Windows XP	V1.0	30/10/2002	01
---	--	------	------------	----

Windows 2000

Références

I	Microsoft Windows 2000 Network Architecture Guide	V1.0	19/04/2001	01
I	Group Policy Reference	V1.08	02/03/2001	04

Systèmes

G	Guide to Securing Microsoft Windows 2000 Group Policy	V1.1	13/11/2001	02
I	Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool	V1.1	22/01/2002	03
P	Guide to Securing Microsoft Windows 2000 File and Disk Resources	V1.0	19/04/2001	08
P	Guide to Securing Microsoft Windows 2000 DNS	V1.0	09/04/2001	06
P	Guide to Securing Microsoft Windows 2000 Encrypting File System	V1.0	01/01/2001	07
P	Guide to Windows 2000 Kerberos Settings	V1.1	27/06/2001	16
P	Microsoft Windows 2000 Router Configuration Guide	V1.02	01/05/2001	17
R	Guide to Securing Windows NT/9x Clients in a Windows 2000 Network	V1.03	06/03/2002	10

Annuaire

I	Guide to Securing Microsoft Windows 2000 Schema	V1.0	06/03/2001	09
I	Guide to Securing Microsoft Windows 2000 Active Directory	V1.0	01/12/2000	05

Certificats

R	Guide to the Secure Config. & Admin. of Microsoft W2K Certificate Services	V2.11	10/10/2001	12
R	Guide to the Secure Config. & Admin. of Microsoft W2K Certificate Services (check)	V2.02	10/10/2001	13
R	Guide to Using DoD PKI Certificates in Outlook 2000	V3.1	08/04/2002	15

Services annexes

I	Guide to Secure Configuration & Administration of Microsoft ISA Server 2000	V1.41	07/01/2002	11
P	Guide to the Secure Configuration & Administration of Microsoft IIS 5.0	V1.31	04/03/2002	14
P	Guide to Securing Microsoft Windows 2000 DHCP	V1.2	25/06/2001	18
P	Guide to Securing Microsoft Windows 2000 Terminal Services	V1.0	02/07/2001	19
P	Microsoft Windows 2000 IPsec Guide	V1.0	13/08/2001	20
✓ P	Guide to the Secure Configuration and Administration of Microsoft Exchange 2000	V1.2	24/11/2003	21

Windows NT

P	Guide to Securing Microsoft Windows NT Networks	V4.2	18/09/2001	nt1
---	---	------	------------	-----

Cisco

R	Router Security Configuration Guide, Executive Summary	V1.0c	27/12/2001	cis1
P	Router Security Configuration Guide	V1.1	27/09/2002	cis2

Contenus exécutables

R	E-mail Security in the Wake of Recent Malicious Code Incidents	V2.5	20/08/2001	eec1
P	Guide to the Secure Configuration and Administration of Microsoft Exchange 5	V3.0	07/01/2002	eec2
R	Microsoft Office 97 Executable Content Security Risks and Countermeasures	V1.1	20/12/1999	eec3
R	Microsoft Office 2000 Executable Content Security Risks and Countermeasures	ND	08/02/2002	eec4

Documents de Support

I	Defense in Depth	ND	ND	sd01
P	Guide to the Secure Configuration & Administration of iPlanet Web Serv Ent. Ed. 4.1	V1.73	03/07/2001	sd02
P	Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0	V1.33	04/03/2002	sd03
P	Guide to the Secure Conf. and Admin. of Microsoft IIS 4.0 (Checklist Format)	V1.33	04/03/2002	sd04
P	Secure Config. of the Apache Web Server, Apache Server V1.3.3 on Red Hat Linux 5.1	V1.12	24/04/2001	sd05
R	Microsoft NetMeeting 3.0 Security Assessment and Configuration Guide	V1.14	05/10/2001	sd06
R	The 60 Minute Network Security Guide	V1.1	18/02/2002	sd07
R	Guide to Securing Microsoft Internet Explorer 5.5 Using Group Policy	V1.0	07/2002	sd08
R	Guide to the Secure Configuration and Administration of Microsoft SQL Server 2000	V1.5	15/01/2003	sd09
R	Guide to Securing Netscape Navigator 7.0	V1.0	02/2002	sd10
R	Guide to the Secure Configuration and Administration of Oracle9i	V1.2	30/10/2003	sd11

• Complément d'information

<http://nsa1.www.conxion.com/>

- Accès aux guides

CRYPTOGRAPHIE

CHALLENGE RSA-576

• Description

En 1991, la société **RSA Security** lançait à la communauté des cryptanalystes une série de 41 défis intitulés '**RSA Factoring challenge**' dont l'objectif consistait en la factorisation – réduction sous la forme des deux facteurs premiers - de nombres dont la longueur s'échelonnait de 100 à 500 chiffres par pas de 10 chiffres. Par le passé, cinq de ces défis ont été remportés dont **RSA-129**, **RSA-130**, **RSA-140** (terminé le 2/02/1999), **RSA-155** (terminé le 22/08/1999) et tout dernièrement **RSA-160** (terminé le 01/04/2003).

Mi-Mai 2001, la société **RSA Security** annonçait la continuation de la série de défis '**RSA Factoring challenge**' sous une nouvelle forme en offrant une dotation allant de \$10 000 à \$200 000 avec l'ouverture de huit nouveaux défis (Rapport N° 34 – Mai 2001).

Le 3 décembre, l'équipe de l'université de **Bonn** ayant emporté le dernier défi de la première série annonçait avoir réussi à factoriser le premier défi de la nouvelle série, à savoir un nombre de 576 bits c'est à dire constitué de 174 chiffres décimaux.

A l'heure de l'écriture de cet article, aucune information précise concernant la durée de la factorisation et la puissance de calcul requise n'est disponible. Le message transmis par l'équipe indique seulement que la méthode de crible dite '**General Number Field Sieve**' ou '**GNFS**' a encore une fois été employée avec succès. Sept défis de la nouvelle série restent à ce jour ouverts à qui souhaite tenter sa chance :

Défi	Date	Taille	Durée
RSA-100	1991	NA	NA
RSA-110	1992	NA	NA
RSA-120	1993	NA	NA
RSA-129	1977	426 bits	32 sem.
RSA-130	1996	428 bits	33 sem.
RSA-140	1999	465 bits	9 sem.
RSA-155	1999	512 bits	30 sem.
RSA-160	2003	540 bits	2 sem.
RSA-576	2003	576 bits	? sem.

Défi	Prix	Digits	Nombre à factoriser
RSA-640	\$ 20 000	193	3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838033415471073108501919548529007337724822783525742386454014691736602477652346609
RSA-704	\$ 30 000	212	74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359
RSA-768	\$ 50 000	232	1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413
RSA-896	\$ 75 000	270	412023436986659543855531365332575948179811699844327982845455626433876445565248426198098870423161841879261420247188869492560931776375033421130982397485150944909106910269861031862704114880866970564902903653658867433731720813104105190864254793282601391257624033946373269391
RSA-1024	\$100 000	309	135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563
RSA-1536	\$150 000	463	1847699703211741474306835620200164403018549338663410171471785774910651696711161249859337684305435744585616061544571794052229717732524660960646946071249623720442022269756756687378427562389508764678440933285157496578843415088475528298186726451339863364931908084671990431874381283363502795470282653297802934916155811881049844908319545009848393775227257052578591944993870073695755688436933812779613089230392569695253261620823676490316036551371447913932347169566988069

RSA-2048	\$200 000	617	251959084756578934940271832400483985714292821262040320277713783604366202070759555 6264018525880784406918290641249515082189298559149176184502808489120072844992687392 8072877767359714183472702618963750149718246911650776133798590957000973304597488084 2840179742910064245869181719511874612151517265463228221686998754918242243363725908 5141865462043576798423387184774447920739934236584823824281198163815010674810451660 3773060562016196762561338441436038339044149526344321901146575444541784240209246165 1572335077870774981712577246796292638635637328991215483143816789988504044536402352 7381951378636564391212010397122822120720357
-----------------	-----------	-----	--

On notera que l'une des opérations de crible a été partiellement prise en charge par la grille de calcul distribuée 'NSFNET' actuellement activée sur la validation de la primalité du nombre de Mersenne **M811** prenant la forme ' $2^{811}-1$ '.

Rappelons à ce propos, que le plus grand nombre premier connu à ce jour a été découvert le 2 décembre par l'un des 60 000 systèmes privés participant à la grille de calcul 'GIMPS' (Great Internet Mersenne Prime Search). Il s'agit du nombre de Mersenne **M20996011** ($2^{20996011}-1$) constitué de quelques 6 320 430 chiffres.

▪ **Complément d'information**

<http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html>

<http://www.loria.fr/~zimmerma/records/rsa576>

<http://www.nfsnet.org/faq-nfs.html>

<http://www.cybersciences.com/Cyber/3.0/N3344.asp>

- Présentation des défis RSA

- Annonce de la factorisation

- Foire aux questions

- Le plus grand nombre premier

LA LEGISLATION

SECURITE

EU - CREATION DE L'AGENCE EUROPEENNE CHARGEE DE LA SECURITE DES RESEAUX ET DE L'INFORMATION

▪ **Description**

Le 19 novembre dernier, le Parlement Européen a adopté le texte de règlement officialisant la création de l'agence européenne chargée de la sécurité des réseaux et de l'information.

L'adoption de ce texte vient confirmer la volonté de la Communauté Européenne d'améliorer sa capacité à traiter les problèmes de sécurité. Le communiqué de presse publié sur le site gouvernemental de la sécurité des systèmes d'information précise que cette agence n'a pas pour vocation le traitement au jour le jour des incidents informatiques lesquels seront traités par les équipes nationales existantes de réponse aux incidents. Elle sera plus particulièrement chargée de l'analyse des risques et de la promotion des actions de prévention des incidents.

▪ **Complément d'information**

<http://www.ssi.gouv.fr/fr/actualites/aecsri.html>

- Communiqué de presse du SSI

LOGICIELS LIBRES

LES SERVICES DE BASE

Les dernières versions des services de base sont rappelées dans les tableaux suivants. Nous conseillons d'assurer rapidement la mise à jour de ces versions, après qualification préalable sur une plate-forme dédiée.

RÉSEAU

Nom	Fonction	Ver.	Date	Source
BIND	Gestion de Nom (DNS)	9.2.3	23/10/03	http://www.isc.org/products/BIND
		8.4.3	24/11/03	
DHCP	Serveur d'adresse	3.0p2	15/01/03	http://www.isc.org/products/DHCP/dhcp-v3.html
NTP4	Serveur de temps	4.2.0	15/10/03	http://www.ntp.org/downloads.html
WU-FTP	Serveur de fichiers	2.6.2p	28/08/03	http://www.wu-ftp.org

MESSAGERIE

Nom	Fonction	Ver.	Date	Source
IMAP4	Relevé courrier	2002e	09/09/03	ftp://ftp.cac.washington.edu/imap/
POP3	Relevé courrier	4.0.5	13/03/03	ftp://ftp.qualcomm.com/eudora/servers/unix/popper/
SENDMAIL	Serveur de courrier	8.12.10	24/09/03	ftp://ftp.sendmail.org/pub/sendmail/RELEASE_NOTES

WEB

Nom	Fonction	Ver.	Date	Source
APACHE	Serveur WEB	1.3.29	24/10/03	http://httpd.apache.org/dist
		2.0.48	24/10/03	
ModSSL	API SSL Apache 1.3.29	2.8.16	01/11/03	http://www.modssl.org
MySQL	Base SQL	3.23.58	11/09/03	http://www.mysql.com/doc/N/e/News-3.23.x.html
		4.0.17	14/10/03	
SQUID	Cache WEB	2.5s4	15/09/03	http://www.squid-cache.org

AUTRE

Nom	Fonction	Ver.	Date	Source
INN	Gestion des news	2.4.0	10/05/03	http://www.isc.org/products/INN
MAJORDOMO	Gestion des listes	1.94.5	15/01/00	http://www.greatcircle.com/majordomo
OpenCA	Gestion de certificats	0.9.1.5	11/12/03	http://www.openca.org/openca/download-releases.shtml
OpenLDAP	Gestion de l'annuaire	2.1.25	06/12/03	ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/

LES OUTILS

Une liste, non exhaustive, des produits et logiciels de sécurité du domaine public est proposée dans les tableaux suivants.

LANGAGES

Nom	Fonction	Ver.	Date	Source
SPLINT	Analyse de code	3.1.1	25/05/03	http://lclint.cs.virginia.edu
Perl	Scripting	5.8.2	05/11/03	http://www.cpan.org/src/index.html
PHP	WEB Dynamique	4.3.4	03/11/03	http://www.php.net/downloads.php
		5.0b3	21/12/03	

ANALYSE RÉSEAU

Nom	Fonction	Ver.	Date	Source
Big Brother	Visualisateur snmp	1.9c	15/05/02	http://bb4.com/
Dsniff	Boîte à outils	2.3	17/12/00	http://www.monkey.org/~dugsong/dsniff
EtterCap	Analyse & Modification	0.6.b	03/07/03	http://ettercap.sourceforge.net/index.php?s=history
Ethereal	Analyse multiprotocole	0.10.0	12/12/03	http://www.ethereal.com
IP Traf	Statistiques IP	2.7.0	19/05/02	http://cebu.mozcom.com/riker/iptraf/
Nstreams	Générateur de règles	1.0.3	06/08/03	http://www.hsc.fr/ressources/outils/nstreams/download/
SamSpade	Boîte à outils	1.14	10/12/99	http://www.samspace.org/ssw/
TcpDump	Analyse multiprotocole	3.8.1	29/12/03	http://www.tcpdump.org/
Libpcap	Acquisition Trame	0.8.1	27/02/02	http://www.tcpdump.org/
TcpFlow	Collecte données	0.21	07/08/03	http://www.circlemud.org/~jelson/software/tcpflow/
TcpShow	Collecte données	1.81	21/03/00	http://ftp7.usa.openbsd.org/pub/tools/unix/sysutils/tcpshow

WinPCap	Acquisition Trame	3.01a	13/06/03	http://winpcap.polito.it/news.htm
---------	-------------------	-------	----------	---

ANALYSE DE JOURNAUX

Nom	Fonction	Ver.	Date	Source
Analog	Journaux serveur http	5.32	23/03/03	http://www.analog.cx
Autobuse	Analyse syslog	1.13	31/01/00	http://www.picante.com/~gtaylor/autobuse
fwLogWatch	Analyse log	0.9.3	23/06/03	http://cert.uni-stuttgart.de/projects/fwlogwatch/
SnortSnarf	Analyse Snort	021111	02/11/02	http://www.silicondefense.com/software/snortsnarf/
WebAlizer	Journaux serveur http	2.01-10	24/04/02	http://www.mrunix.net/webalizer/download.html

ANALYSE DE SÉCURITÉ

Nom	Fonction	Ver.	Date	Source
FIRE	Boîte à outils	0.4a	14/05/03	http://sourceforge.net/projects/biatchux/
curl	Analyse http et https	7.10.8	01/11/03	http://curl.haxx.se/
Nessus	Vulnérabilité réseau	2.0.9	05/11/03	http://www.nessus.org
Nmap	Vulnérabilité réseau	3.48	28/10/03	http://www.insecure.org/nmap/nmap_download.html
Pandora	Vulnérabilité Netware	4.0b2.1	12/02/99	http://www.packetfactory.net/projects/pandora/
Saint	Vulnérabilité réseau	5.1.3	24/12/03	http://www.saintcorporation.com/updates.html
Sara	Vulnérabilité réseau	5.0.0	05/12/03	http://www.www-arc.com/sara/downloads/
Tara (tiger)	Vulnérabilité système	3.0.3	15/08/02	http://www.arc.com/tara
Tiger	Vulnérabilité système	2.2.4p1	19/07/99	ftp://net.tamu.edu/pub/security/TAMU/tiger
Trinix	Boîte à outils	0.89	02/08/01	http://sourceforge.net/projects/trinix/
Whisker	LibWhisker	1.8	26/09/03	http://www.wiretrip.net/rfp/p/doc.asp?id=21

CONFIDENTIALITÉ

Nom	Fonction	Ver.	Date	Source
OpenPGP	Signature/Chiffrement			http://www.openpgp.org
GPG	Signature/Chiffrement	1.2.4	24/12/03	http://www.gnupg.org

CONTRÔLE D'ACCÈS

Nom	Fonction	Ver.	Date	Source
TCP Wrapper	Accès services TCP	7.6		ftp://ftp.cert.org/pub/tools/tcp_wrappers
Xinetd	Inetd amélioré	2.3.12	05/08/03	http://synack.net/xinetd/

CONTRÔLE D'INTÉGRITÉ

Nom	Fonction	Ver.	Date	Source
Tripwire	Intégrité LINUX	2.3.47	15/08/00	http://www.tripwire.org/downloads/index.php
ChkRootKit	Compromission UNIX	0.43	27/12/03	http://www.chkrootkit.org/

DÉTECTION D'INTRUSION

Nom	Fonction	Ver.	Date	Source
Deception TK	Pot de miel	19990818	18/08/99	http://all.net/dtk/index.html
LLNL NID	IDS Réseau	2.6	10/10/02	http://ciac.llnl.gov/cstc/nid/nid.html
Snort	IDS Réseau	2.1.0	18/12/03	http://www.snort.org/dl/
Shadow	IDS Réseau	1.8	30/04/03	http://www.nswc.navy.mil/ISSEC/CID/

GÉNÉRATEURS DE TEST

Nom	Fonction	Ver.	Date	Source
Elza	Requêtes HTTP	1.4.5	01/04/00	http://www.stoev.org/elza/project-news.html
FireWalk	Analyse filtres	5.0	20/10/02	http://www.packetfactory.net/firewalk
IPSend	Paquets IP	2.1a	19/09/97	ftp://coombs.anu.edu.au/pub/net/misc
IDSWakeUp	Détection d'intrusion	1.0	13/10/00	http://www.hsc.fr/ressources/outils/idswakeup/download/
UdpProbe	Paquets UDP	1.2	13/02/96	http://sites.inka.de/sites/bigred/sw/udpprobe.txt

PARE-FEUX

Nom	Fonction	Ver.	Date	Source
DrawBridge	PareFeu FreeBSD	3.1	19/04/00	http://drawbridge.tamu.edu
IpFilter	Filtre datagramme	3.4.33p2	24/11/03	http://coombs.anu.edu.au/ipfilter/ip-filter.html
NetFilter	Pare-Feu IpTables	1.2.9	02/11/03	http://www.netfilter.org/downloads.html

TUNNELS

Nom	Fonction	Ver.	Date	Source
CIPE	Pile Crypto IP (CIPE)	1.5.4	29/06/01	http://sites.inka.de/sites/bigred/devel/cipe.html
FreeSwan	Pile IPSec	2.04	13/11/03	http://www.freeswan.org
http-tunnel	Encapsulation http	3.0.5	06/12/00	http://www.nocrew.org/software/httpunnel.html
OpenSSL	Pile SSL	0.9.7c	30/09/03	http://www.openssl.org/
OpenSSH	Pile SSH 1 et 2	3.7.1	16/09/03	http://www.openssh.com/
Stunnel	Proxy https	4.04	12/01/03	http://www.stunnel.org
TeraTerm Pro	Terminal SSH2	3.1.3	08/10/02	http://www.ayera.com/teraterm/
Zebedee	Tunnel TCP/UDP	2.4.1	29/05/02	http://www.winton.org.uk/zebedee/

NORMES ET STANDARDS

LES PUBLICATIONS DE L'IETF

LES RFC

Du 28/11/2003 au 29/12/2003, 25 RFC ont été publiés dont 5 RFC ayant trait à la sécurité.

RFC TRAITANT DE LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
DHCP	3634	12/03	Pst	KDC Server Address Sub-option for the DHCP CableLabs Client Configuration (CCC) Option
SECUR	3631	12/03	Inf	Security Mechanisms for the Internet
XML	3653	12/03	Inf	XML-Signature XPath Filter 2.0

RFC TRAITANT DE DOMAINES CONNEXES À LA SÉCURITÉ

Thème	Num	Date	Etat	Titre
DNS	3658	12/03	Pst	Delegation Signer (DS) Resource Record (RR)
LDAP	3671	12/03	Pst	Collective Attributes in the Lightweight Directory Access Protocol (LDAP)
	3672	12/03	Pst	Subentries in the Lightweight Directory Access Protocol (LDAP)
	3673	12/03	Pst	Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes
	3674	12/03	Pst	Feature Discovery in Lightweight Directory Access Protocol (LDAP)
	3663	12/03	Exp	Domain Administrative Data in Lightweight Directory Access Protocol (LDAP)

AUTRES RFC

Thème	Num	Date	Etat	Titre
DHCP	3633	12/03	Pst	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
DIFFSERV	3662	12/03	Inf	A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services
DMDP	3656	12/03	Exp	The Mailbox Update (MUPDATE) Distributed Mailbox Database Protocol
DNS	3646	12/03	Pst	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
FC	3643	12/03	Pst	Fibre Channel (FC) Frame Encapsulation
IETF	3299	12/03	Inf	Request for Comments Summary RFC Numbers 3200-3299
	3499	12/03	Inf	Request for Comments Summary RFC Numbers 3400-3499
	3599	12/03	Inf	Request for Comments Summary RFC Numbers 3500-3599
	3677	12/03	BCP	IETF ISOC Board of Trustee Appointment Procedures
MGCP	3660	12/03	Inf	Basic Media Gateway Control Protocol (MGCP) Packages
	3661	12/03	Inf	Media Gateway Control Protocol (MGCP) Return Code Usage
MIB	3621	12/03	Pst	Power Ethernet MIB
SIP	3665	12/03	BCP	Session Initiation Protocol (SIP) Basic Call Flow Examples
	3666	12/03	BCP	Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows
TCP	3649	12/03	Exp	HighSpeed TCP for Large Congestion Windows
WEBDAV	3648	12/03	Pst	Web Distributed Authoring and Versioning (WebDAV) Ordered Collections Protocol

LES DRAFTS

Du 28/11/2003 au 29/12/2003, 258 drafts ont été publiés: 188 drafts mis à jour, 70 nouveaux drafts, dont 10 drafts ayant directement trait à la sécurité.

NOUVEAUX DRAFTS TRAITANT DE LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
CRYPTO	draft-paddon-sober128-00	02/12	SOBER-128: A Fast Stream Cipher with Simultaneous MAC
EAP	draft-yanagiya-eap-saa-00	03/12	Service Authentication Architecture Using EAP Key
HTTP	draft-melnikov-http-auth-url-00	23/12	HTTP URL Scheme extension for authentication
IKE	draft-hoffman-pki4ipsec-profile-00	23/12	Profile for Certificate Use in IKE version 1
IPSEC	draft-ietf-ipsec-esp-ah-algorithms-00	18/12	Cryptographic Algorithm Implementation requ. for ESP And AH
NEMO	draft-petrescu-nemo-threats-00	02/12	Threats for Basic Network Mobility Support (NEMO threats)
MSEC	draft-ietf-msec-ipsec-signatures-00	04/12	The Use of RSA Signatures within ESP and AH
RADIUS	draft-lior-radius-attribute-type-extension-00	18/12	RADIUS Attribute Type Extension
SPAM	draft-stout-antispam-00	04/12	Anti-Spam Recommendations II for SMTP MTAs
SSH	draft-stebila-secsh-ecdh-00	02/12	EC Diffie-Hellman Key Exchange for SSH Transport Level Protocol

MISE À JOUR DE DRAFTS TRAITANT DE LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
CGA	draft-ietf-send-cga-04	18/12	Cryptographically Generated Addresses (CGA)
CMS	draft-ietf-smime-pss-03	19/12	Use of the PSS Signature Algorithm in CMS
COPS	draft-vatiainen-mcop-cops-01	17/12	Multicast Control Protocol (MCOP) over COPS
CRYPTO	draft-eastlake-randomness2-05	09/12	Randomness Requirements for Security
	draft-nakajima-camellia-03	15/12	A Description of the Camellia Encryption Algorithm
	draft-orman-public-key-lengths-06	01/12	Determining Strengths For Public Keys used For Exchanging ...
DNS	draft-ietf-dnsext-dnssec-intro-08	18/12	DNS Security Introduction and Requirements
	draft-ietf-dnsext-dnssec-protocol-04	18/12	Protocol Modifications for the DNS Security Extensions
	draft-ietf-dnsext-dnssec-records-06	18/12	Resource Records for DNS Security Extensions
	draft-ietf-dnsext-keyrr-key-signing-flag-12	18/12	KEY RR Secure Entry Point Flag
	draft-ietf-dnsext-nsec-rdata-03	22/12	DNSSEC NSEC RDATA Format
EAP	draft-ietf-eap-rfc2284bis-07	02/12	Extensible Authentication Protocol (EAP)
ECDSA	draft-blake-wilson-xmldsig-ecdsa-07	19/12	ECDSA with XML-Signature Syntax
EDI	draft-ietf-ediint-as2-14	01/12	MIME Secure P2P Business Data Interchange using HTTP AS2
HEALTH	draft-marshall-security-audit-08	16/12	Security Audit & Access Accountability Message XML Data ...
IMAP	draft-siemborski-imap-sasl-initial-response-02	05/12	IMAP Extension for SASL Initial Client Response
IPS	draft-ietf-ips-auth-mib-05	10/12	Definitions of Managed Objects for User Identity Authentication
IPSEC	draft-ietf-ipseckey-rr-08	16/12	A method for storing IPsec keying material in DNS
IPV4	draft-ietf-v6ops-ipv4survey-sec-04	22/12	Survey of IPv4 addr in Currently Deployed IETF Security Area Std
LDAP	draft-ietf-ldapbis-authmeth-09	11/12	LDAP: Auth. Methods and Connection Level Security Mechanism
MIKEY	draft-ietf-msec-mikey-08	16/12	MIKEY: Multimedia Internet KEYing
MOBILEIP	draft-carroll-dynmobileip-cdma-03	04/12	Wireless Dynamic Mobile IP Key Update for cdma2000 Networks
	draft-nikander-mobileip-v6-ro-sec-02	04/12	Mobile IP version 6 Route Optimization Security Design Backg.
	draft-ietf-mip4-aaa-nai-02	16/12	Mobile IPv4 Extension for AAA Network Access Identifiers
MPLS	draft-behringer-mpls-security-05	02/12	Analysis of the Security of BGP/MPLS IP VPNs
OPES	draft-ietf-opes-threats-03	10/12	Security Threats and Risks for Open
OPSEC	draft-jones-opsec-03	16/12	Operational Security Requirements for IP Network Infrastructure
PKIX	draft-ietf-pkix-acpolicies-extn-05	04/12	Attribute Certificate Policies extension
	draft-ietf-pkix-certpathbuild-02	02/12	Internet X.509 PKI: Certification Path Building
	draft-ietf-pkix-logotypes-13	03/12	Internet X.509 PKI: Logotypes in X.509 certificates
	draft-ietf-pkix-proxy-10	23/12	Internet X.509 PKI Proxy Certificate Profile
	draft-ietf-pkix-rsa-pkalg-01	02/12	Additional Algorithms & Identifiers for RSA Cryptography
RFC1734	draft-siemborski-rfc1734bis-02	05/12	POP3 SASL Authentication Mechanism
RFC2554	draft-siemborski-rfc2554bis-02	05/12	SMTP Service Extension for Authentication
SASL	draft-ietf-sasl-crammd5-01	01/12	The CRAM-MD5 SASL Mechanism
SCEP	draft-ietf-sasl-rfc2222bis-04	23/12	Simple Authentication and Security Layer (SASL)
	draft-nourse-scep-09	09/12	Cisco Systems' Simple Certificate Enrollment Protocol(SCEP)
SECURITY	draft-yang-scxp-01	03/12	The Security Components Exchange Protocol(SCXP)
	draft-ietf-rpsec-routing-threats-04	18/12	Generic Threats to Routing Protocols
SIPP	draft-rosenberg-sipping-nat-scenarios-02	04/12	NAT and Firewall Scenarios and Solutions for SIP
TLS	draft-friend-tls-lzs-compression-01	16/12	Transport Layer Security Protocol Compression Using LZS

DRAFTS TRAITANT DE DOMAINES CONNEXES À LA SÉCURITÉ

Thème	Nom du Draft	Date	Titre
AAA	draft-ietf-aaa-diameter-cc-02	18/12	Diameter Credit-control Application
BMWG	draft-ietf-bmwg-ospfconv-intraarea-07	05/12	Benchmarking OSPF Single Router Control Plane Convergence
DHC	draft-daniel-dhc-dhcpv6-ctep-opt-01	18/12	Configured Tunnel End Point Option for DHCPv6
L2TP	draft-townesley-l2tpv3-mpls-01	04/12	Encapsulation of MPLS over Layer 2 Tunneling Protocol Version 3
LDAP	draft-ietf-ldapbis-protocol-19	03/12	LDAP: The Protocol
	draft-legg-ldap-transfer-02	22/12	LDAP: Transfer Encoding Options
	draft-sciabarras-xed-eldif-01	19/12	The Extended LDAP Data Interchange Format (ELDIF)
	draft-sermersheim-ldap-csn-00	08/12	The LDAP Change Sequence Number Syntax and Matching Rules
MPLS	draft-behringer-mpls-vpn-auth-03	02/12	MPLS VPN Import/Export Verification
	draft-hsmit-mpls-igp-spf-01	10/12	Calculating IGP routes over Traffic Engineering tunnels
OSPF	draft-ietf-ospf-2547-dnbit-02	04/12	Using an LSA Options Bit to Prevent Looping in BGP/MPLS IP VPNs
	draft-mirtorabi-ospf-tunnel-adjacency-01	16/12	OSPF Tunnel Adjacency
PPP	draft-tacsik-pppext-ipcp-opt-ipv6-sip-pro-00	05/12	IPv6CP option for IPv6 SIP Proxy address
	draft-tacsik-pppext-ipv6cp-opt-sip-proxy-00	18/12	IPv6CP option for SIP Proxy address
RPSL	draft-blunk-rpsl-02	04/12	Routing Policy Specification Language next generation (RPSLNg)
SYSLOG	draft-ietf-syslog-protocol-00	03/12	The syslog Protocol
UDDI	draft-bergeson-uddi-ldap-schema-02	18/12	Ldap Schema for UDDI
VPN	draft-groom-vpn-tunnel-00	05/12	VPN Performance Measurements – an open model based proposal
XCON	draft-ietf-xcon-cpcp-reqs-00	08/12	Requirements for Conference Policy Control Protocol

AUTRES DRAFTS

Thème	Nom du Draft	Date	Titre
AVT	draft-jones-avt-audio-t38-03	03/12	Real-Time Facsimile - audio/t38 MIME Sub-type Registration
BCP38	draft-savola-bcp38-multihoming-update-03	23/12	Ingress Filtering for Multihomed Networks
BGP	draft-ietf-grow-bgp-med-considerations-00	03/12	BGP MED Considerations
	draft-ietf-grow-collection-communities-01	15/12	BGP Communities for Data Collection

	draft-ietf-grow-embed-addr-00	03/12	Embedding Globally Routable Internet addr Considered Harmful
CAPWAP	draft-calhoun-capwap-problem-statement-01	01/12	CAPWAP Problem Statement
CHECK	draft-nunzi-check-mib-00	22/12	Definitions of Managed Objects for the Health Check Operations
DHCP	draft-hibbs-dhc-changes-00	04/12	Requirements for Proposed Changes to DHCP for IPv4
	draft-ietf-dhc-dhcpv6-opt-nisconfig-05	03/12	NIS Configuration Options for DHCPv6
	draft-ietf-dhc-dhcpv6-stateless-03	23/12	A Guide to Implementing Stateless DHCPv6 Service
	draft-ietf-dhc-failover-12	03/12	DHCP Failover Protocol
	draft-ietf-dhc-rapid-commit-opt-00	02/12	Rapid Commit Option for DHCPv4
	draft-ietf-dhc-server-mib-09	02/12	Dynamic Host Configuration Protocol for IPv4 Server MIB
	draft-ietf-dhc-subscriber-id-04	18/12	DHCP Subscriber ID Suboption for the DHCP Relay Agent Option
	draft-vijay-dhc-dhcpv6-ipv6trans-00	03/12	DHCPv6 support for IPv6 Transition
DMP	draft-fecyk-dmp-01	18/12	Designated Mailers Protocol
DNS	draft-ietf-dnsext-dnssec-2535type-change-06	16/12	Legacy Resolver Compatibility for Delegation Signer
	draft-ietf-dnsext-mdns-27	18/12	Linklocal Multicast Name Resolution (LLMNR)
	draft-ietf-dnsop-ipv6-dns-issues-03	04/12	Operational Considerations and Issues with IPv6 DNS
DOCIS	draft-ietf-ipcdn-docs-rfmbv2-09	19/12	RF Interface MIB for DOCSIS 2.0 compliant RF interfaces
DYN	draft-royer-dyn-query-00	23/12	Variables in Dynamic Queries for iCalendar
EAP	draft-urien-eap-ssc-01	22/12	EAP-SSC Secured Smartcard Channel
ENUM	draft-ietf-enum-pres-00	18/12	Enumservice Registration for Presence Services
	draft-ietf-enum-sip-01	01/12	enumservice registration for SIP Addresses-of-Record
EPP	draft-hollenbeck-epp-rgp-02	17/12	Redemption Grace Period Mapping for Ext Provisioning Protocol
	draft-zygmuntowicz-epp-pltld-01	01/12	EPP parameters for .pl ccTLD
FAX	draft-ietf-fax-esmtp-conneg-09	05/12	SMTP and MIME Extensions For Content Conversion
FORCES	draft-draft-ietf-forces-evaluation-00	10/12	ForCES Protocol Evaluation Draft
	draft-ietf-forces-evaluation-00	10/12	ForCES Protocol Evaluation Draft
	draft-ietf-forces-framework-12	18/12	Forwarding and Control Element Separation (ForCES) Framework
GBP	draft-ietf-idr-bgp4-23	02/12	A Border Gateway Protocol 4 (BGP-4)
	draft-ietf-idr-bgp-identifier-03	03/12	AS-wide Unique BGP Identifier for BGP-4
GEOPRIV	draft-ietf-geopriv-dhcp-lci-option-03	09/12	DHCP Option for Coordinate-based Location Configuration Info.
HTTP	draft-gettys-http-v11-spec-rev-00	03/12	Hypertext Transfer Protocol -- HTTP/1.1
IDMR	draft-ietf-idmr-dvmrp-v3-11	03/12	Distance Vector Multicast Routing Protocol
IETF	draft-iab-advcomm-00	01/12	The IETF in the Large: Administration and Execution
	draft-iab-liaison-mgt-00	01/12	IAB Processes for management of liaison relationships
	draft-meyer-wg-post-meeting-00	23/12	IETF Session Minutes and Presentation Materials
	draft-mrose-ietf-posting-04	02/12	A Practice for Revoking Posting Rights to IETF mailing lists
IMAP	draft-gellens-lemonade-push-00	10/12	IMAP Message Submission
	draft-ietf-imapext-condstore-05	01/12	IMAP Extension for Conditional STORE operation
	draft-ietf-imapext-sort-14	04/12	IMAP - SORT AND THREAD EXTENSION
	draft-ietf-lemonade-catenate-00	08/12	Internet Message Access Protocol (IMAP) CATENATE Extension
IP	draft-fair-ipdvb-req-04	17/12	Requirements for transmission of IP datagrams over MPEG-2 net
	draft-fenner-traceroute-ipm-00	04/12	A 'traceroute' facility for IP Multicast.
IPFIX	draft-ietf-ipfix-info-02	03/12	Information Model for IP Flow Information Export
IPOIB	draft-ietf-ipoib-ip-over-infiniband-05	01/12	Transmission of IP over InfiniBand
IPSEC	draft-ietf-ipsec-ikev2-iana-00	18/12	Initial IANA registry contents
IPTEL	draft-ietf-ieprep-ets-telephony-07	02/12	IP Telephony reqs for Emergency Telecommunication Service
	draft-ietf-ieprep-framework-07	03/12	Framework for Supporting IEPS in IP Telephony
IPv4	draft-ietf-v6ops-ipv4survey-apps-04	22/12	Survey of IPv4 Addr in Currently Deployed IETF Application Area
	draft-ietf-v6ops-ipv4survey-intro-06	22/12	Intro. to the Survey of IPv4 Addr in Currently Deployed IETF Std
	draft-ietf-v6ops-ipv4survey-ops-05	22/12	Survey of IPv4 Addr in Currently Deployed IETF Operations & M..
	draft-ietf-v6ops-ipv4survey-routing-03	05/12	Survey of IPv4 Addr in Currently Deployed IETF Routing Area Std
	draft-ietf-v6ops-ipv4survey-subip-04	01/12	Survey of IPv4 Addr in Currently Deployed IETF Sub-IP Area Std
	draft-ietf-v6ops-ipv4survey-trans-05	04/12	Survey of IPv4 Addr in Currently Deployed IETF Transport Area
	draft-ietf-v6ops-ipv6-scenarios-analysis-00	05/12	Scenarios and Analysis for Introducing IPv6 into ISP Networks
	draft-nickless-ipv4-mcast-unusable-03	08/12	IPv4 Multicast Unusable Group And Source Addresses
IPv6	draft-dupont-ipv6-imei-06	16/12	IMEI-based universal IPv6 interface IDs
	draft-hain-templin-ipv6-localcomm-04	09/12	Goals for Organizational-Scope Communications
	draft-ietf-imss-ipv6-over-fibre-channel-01	04/12	Transmission of IPv6 Packets over Fibre Channel
	draft-ietf-ipv6-flow-label-09	16/12	IPv6 Flow Label Specification
	draft-ietf-ipv6-node-requirements-07	10/12	IPv6 Node Requirements
	draft-ietf-ipv6-rfc2012-update-05	01/12	Management Information Base for the TCP
	draft-ietf-ipv6-router-selection-03	18/12	Default Router Preferences, More-Specific Routes & Load Sharing
	draft-jfaizan-mip6-vhar-00	18/12	Virtual Home Agent Reliability Protocol (VHAR)
	draft-ooms-v6ops-bgp-tunnel-01	22/12	Connecting IPv6 Islands across IPv4 Clouds with BGP
	draft-paakkonen-addressing-htr-manet-00	10/12	IPv6 addressing in a heterogeneous MANET-network
	draft-park-dna-ipv6dadopt-requirement-02	02/12	IPv6 DAD Optimization Goals and Requirements
ISIS	draft-ietf-isis-experimental-tlv-01	10/12	TLV for Experimental Use
	draft-ietf-isis-ip-interoperable-02	10/12	Recommendations for Interoperable IP Networks using IS-IS
	draft-ietf-isis-iso-interoperable-02	15/12	Recommendations for Interoperable Networks using IS-IS
L2TP	draft-dasilva-l2tp-relaysvc-08	04/12	L2TP Active Discovery Relay for PPPoE
LMP	draft-ietf-ccamp-lmp-test-sonet-sdh-04	16/12	SONET/SDH Encoding for LMP Test messages
	draft-ietf-ccamp-lmp-wdm-03	16/12	LMP for DWDM Optical Line Systems
MBONED	draft-ietf-mboned-ipv4-mcast-unusable-01	10/12	IPv4 Multicast Unusable Group And Source Addresses
	draft-lehtonen-mboned-mcop-operation-01	17/12	MCOP operation for first hop routers
MIDCOM	draft-stiemerling-midcom-server-mib-00	03/12	Definitions of Managed Objects for MIDCOM Server
MLD	draft-vida-ml-d-v2-08	03/12	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
MLPP	draft-baker-tsvwg-mlf-concerns-00	02/12	MLEF Considered Harmful
	draft-baker-tsvwg-mlpp-that-works-00	02/12	Implementing MLPP in the Internet Protocol Suite

MMUSIC	draft-ietf-mmusic-anat-00	15/12	The Alternative Network Address Types Semantics for Session ..
	draft-ietf-mmusic-img-framework-02	23/12	A Framework for the Usage of Internet Media Guides
	draft-ietf-mmusic-img-req-02	23/12	Protocol Requirements for Internet Media Guides
	draft-luoma-mmusic-img-metadata-03	22/12	Internet Media Guide Metadata Baseline
	draft-luoma-mmusic-img-metadata-envel-00	10/12	A Metadata Framework for Internet Media Guides: Metadata Env.
	draft-luoma-mmusic-img-muppet-04	16/12	Internet Media Guide Unidirectional Point-to-Multipoint Transport
	draft-srikantan-mmusic-rtsp-streaming-rel-00	04/12	Streaming Relays
MOBILEIP	draft-ietf-mip4-experimental-messages-00	09/12	Experimental Message, Extension and Error Codes for Mobile IPv4
MPLS	draft-boyle-tewg-interarea-reqts-01	15/12	Reqs for support of Inter-Area and Inter-AS MPLS Traffic Eng.
	draft-farrel-mpls-preemption-interim-00	02/12	Interim Report on MPLS Pre-emption
	draft-ietf-ccamp-crankback-00	16/12	Crankback Signaling Extensions for MPLS Signaling
	draft-ietf-ccamp-gmpls-ason-reqts-05	01/12	Requirements for GMPLS Signaling Usage & Extensions for ASON
	draft-ietf-ccamp-gmpls-ason-routing-reqts-01	23/12	Requirements for GMPLS Routing for ASON
	draft-ietf-ccamp-gmpls-rsvp-te-ason-00	10/12	GMPLS RSVP-TE Signalling in support of ASON
	draft-ietf-mpls-p2mp-requirement-00	04/12	Requirements for Point to Multipoint extension to RSVP-TE
	draft-ietf-mpls-rsvpte-attributes-01	18/12	Encoding of Attributes for MPLS LSP Establishment Using RSVP-TE
	draft-ietf-tewg-interas-mpls-te-req-03	10/12	MPLS Inter-AS Traffic Engineering requirements
	draft-martini-l2circuit-trans-mpls-13	09/12	Transport of Layer 2 Frames Over MPLS
	draft-rosen-mpls-explicit-null-01	19/12	Removing a Restriction on the use of MPLS Explicit NULL
	draft-shen-mpls-ldp-nnhop-label-00	04/12	Discovering LDP Next-NextHop Labels
	draft-shen-nhop-fastreroute-00	02/12	NextHop Fast ReRoute for IP and MPLS
	draft-xushao-ipo-mplsovergmpls-01	23/12	Requirements for MPLS over GMPLS-based Optical Networks
MSEC	draft-ietf-msec-mikey-dhmac-05	04/12	HMAC-authenticated Diffie-Hellman for MIKEY
MSGHEAD	draft-newman-msgheader-origininfo-05	28/05	Originator-Info Message Header
MULTI6	draft-lear-multi6-things-to-think-about-00	15/12	Things MULTI6 Developers should think about
NAT	draft-ietf-nat-natmib-08	02/12	Definitions of Managed Objects for Network Address Translators
NEMO	draft-ietf-nemo-basic-support-02	23/12	Nemo Basic Support Protocol
NFS	draft-callaghan-nfsrdmareq-00	11/12	NFS RDMA Requirements
NLTP	draft-jeong-nsis-mobility-ntlp-01	02/12	Mobility Functions in the NLTP
NOID	draft-templin-isnoid-01	03/12	Operation of the NOID Multihoming Protocol on ISATAP Nodes
OCSF	draft-deacon-lightweight-ocsp-profile-00	01/12	Lightweight OCSF Profile for High Volume Environments
OPES	draft-ietf-opes-end-comm-06	09/12	OPES entities and end points communication
	draft-ietf-opes-iab-04	04/12	OPES Treatment of IAB Considerations
	draft-ietf-opes-ocp-core-04	17/12	OPES Callout Protocol Core
OSPF	draft-ietf-ospf-ospfv3-auth-04	11/12	Authentication/Confidentiality for OSPFv3
PANA	draft-yacine-pana-snmp-00	23/12	PANA: SNMP usage for PAA-2-EP interface
PDF	draft-zilles-pdf-01	18/12	The application/pdf Media Type
PILC	draft-ietf-pilc-link-design-15	18/12	Advice for Internet Subnetwork Designers
PKIX	draft-ietf-pkix-sha244-02	18/12	A 224-bit One-way Hash Function: SHA-224
PWE3	draft-stein-pwe3-tdm-packetloss-01	02/12	Effect of Packet Loss on Voice Quality for TDM over Pseudowires
	draft-ietf-pwe3-atm-encap-04	16/12	Encap. Meth for Trans. of ATM Cells/Frame Over IP and MPLS Net
	draft-ietf-pwe3-cep-mib-04	23/12	SONET/SDH CEP Management Information Base Using SMIv2
	draft-ietf-pwe3-control-protocol-05	16/12	Pseudowire Setup and Maintenance using LDP
	draft-ietf-pwe3-enet-mib-03	23/12	Ethernet Pseudo Wire (PW) Management Information Base
	draft-ietf-pwe3-ethernet-encap-05	16/12	Encapsulation Methods for Transport of Eth Frames Over IP/MPLS
	draft-ietf-pwe3-fragmentation-04	09/12	PWE3 Fragmentation and Reassembly
	draft-ietf-pwe3-pw-mpls-mib-04	23/12	Pseudo Wire (PW) over MPLS PSN Management Information Base
	draft-ietf-pwe3-tdm-requirements-03	23/12	Reqs for Edge-to-Edge Emulation of TDM Circuits over PSN
RADIO	draft-aleksandrov-radio-and-television-pro-00	03/12	Radio and Television Protocol
RFC3291	draft-ietf-ops-rfc3291bis-02	03/12	Textual Conventions for Internet Network Addresses
RMON	draft-ietf-rmonmib-raqmon-framework-04	01/12	Real-time Application Quality of Service Monitoring Framework
	draft-ietf-rmonmib-raqmon-mib-03	01/12	Real-time Application Quality of Service Monitoring MIB
	draft-ietf-rmonmib-raqmon-pdu-04	01/12	Real-time Application Quality of Service Monitoring PDU
	draft-ietf-rmonmib-rmon-oid-assignments-01	02/12	IANA guidelines for the registry of rmon MIB modules
RMR	draft-wei-rmr-01	15/12	Remote Multicast Replication (RMR) Protocol
RMT	draft-ietf-rmt-flute-07	15/12	FLUTE - File Delivery over Unidirectional Transport
ROHC	draft-ietf-rohc-mib-rtp-08	03/12	Definitions of Managed Objects for Robust Header Compression
	draft-ietf-rohc-sigcomp-impl-guide-02	23/12	Implementer's Guide for SigComp
	draft-ietf-rohc-sigcomp-nack-00	11/12	A Negative Acknowledgement Mech. for Signaling Compression
	draft-ietf-rohc-udp-lite-02	18/12	ROHC Header Compression (ROHC):Profiles for UDP-Lite
ROUTING	draft-irtf-routing-reqs-02	03/12	Requirements for Inter Domain Routing
RSVP	draft-arun-praba-rsvpte-hello-state-00	01/12	RSVP Hello State machine
	draft-ietf-ccamp-rsvp-te-exclude-route-01	04/12	Exclude Routes - Extension to RSVP-TE
RTP	draft-ietf-avt-ilbc-codec-04	03/12	Internet Low Bit Rate Codec
	draft-ietf-avt-rtp-clearmode-04	05/12	RTP payload format for a 64 kbit/s transparent call
	draft-ietf-avt-rtp-ilbc-04	02/12	RTP Payload Format for iLBC Speech
	draft-ietf-avt-text-red-00	18/12	Registration of the text/red MIME Sub-Type
SCTP	draft-ietf-tsvwg-prsctp-02	01/12	SCTP Partial Reliability Extension
	draft-ietf-tsvwg-sctpimpguide-10	03/12	Stream Control Transmission Protocol (SCTP) Implementors Guide
SEAMOB	draft-ietf-seamoby-mobility-terminology-05	02/12	Mobility Related Terminology
SIEVE	draft-homme-sieve-variables-02	11/12	Sieve -- Variables Extension
	draft-madanganeshv-sieve-remove-attach-00	23/12	SIEVE: Remove attachment(s)
	draft-madanganeshv-sieve-stat-00	03/12	SIEVE Statistics
SIGTRAN	draft-ietf-sigtran-sua-16	16/12	Signalling Connection Control Part User Adaptation Layer (SUA)
SILC	draft-riikonen-flags-payloads-04	03/12	SILC Message Flag Payloads
SIP	draft-elmalki-sipping-3gpp-translator-00	04/12	IPv6-IPv4 Translation mechanism for SIP-based services in 3GPP
	draft-ietf-sip-callee-caps-02	11/12	Indicating User Agent Capabilities in SIP

	draft-ietf-sipping-aaa-req-04	16/12	AAA Requirements for the Session Initiation Protocol
	draft-ietf-sipping-mwi-04	15/12	A Message Summary and Waiting Ind. Event Package for SIP
	draft-rosenberg-sip-gruu-01	08/12	Obtaining & Using Globally Routable User UA URIs (GRUU) in SIP
SLBRP	draft-woolman-slbrp-00	08/12	Server Load Balancing Registration Protocol
SMI	draft-irtf-nmrg-sming-snmpp-05	17/12	SMIng Mappings to SNMP
SMLT	draft-lapuh-network-smlt-03	04/12	Split Multi-link Trunking (SMLT)
SMP	draft-irtf-nmrg-sming-07	17/12	SMIng - Next Generation Structure of Management Information
SMTP	draft-hoffman-utf8headers-00	16/12	SMTP Service Extensions or Transmission of Headers in UTF-8
	draft-malamud-no-soliciting-02	02/12	A 'No Soliciting' SMTP Service Extension
SNMP	draft-chisholm-snmpp-infomode-01	23/12	The SNMP Information Model
	draft-irtf-nmrg-snmpp-getrange-00	02/12	GetRange Operation for the Simple Network Management Protocol
SPAM	draft-yerazunis-spamfilt-inoculation-01	01/12	A MIME Encoding for Spam Inoculation Messages
TCP	draft-allman-tcp-early-rexmt-03	23/12	Early Retransmit for TCP and SCTP
TCP	draft-ietf-rserpool-tcpmapping-01	23/12	TCP Mapping for Reliable Server Pooling Failover Mode
UMSP	draft-bogdanov-umsp-web-00	02/12	Integration of Unified Memory Space Protocol and Web Browser
UNICODE	draft-faltstrom-unicode-synchronisation-00	02/12	Synchronization of Stringprep with Unicode Normalization rules
URI	draft-vandesompele-info-uri-01	05/12	'info' URI Scheme for Information Assets with Identifiers
USEFOR	draft-ietf-usefor-article-12	01/12	News Article Format and Transmission
V6OPS	draft-ietf-v6ops-application-transition-00	10/12	Application Aspects of IPv6 Transition
WAT	draft-srinivas-wat-01	11/12	Web Address Translation (WAT)
WEBDAV	draft-dusseault-caldav-00	18/12	Calendar Server Extensions for WebDAV (CalDAV)
	draft-ietf-webdav-bind-03	15/12	Binding Extensions to Web Distributed Authoring and Versioning
	draft-reschke-webdav-allprop-include-05	04/12	Including additional properties in WebDAV PROPFIND/allprop reqs
XCON	draft-ietf-xcon-conference-scenarios-00	18/12	Conferencing Scenarios
XED	draft-legg-xed-asd-01	22/12	ASN.1 Schema: An XML Representation for ASN.1 Specifications
	draft-legg-xed-glue-01	22/12	XED: Schema Language Integration
	draft-legg-xed-roadmap-02	22/12	The XML Enabled Directory
	draft-legg-xed-schema-01	22/12	XED: Schema Operational Attributes
XML	draft-ietf-xmldsig-xc14n-02	03/12	Exclusive XML Canonicalization, Version 1.0
	draft-legg-xed-rxer-00	22/12	Robust XML Encoding Rules for ASN.1 Types

NOS COMMENTAIRES

LES RFC

RFC 3299/3499/3599

Summary RFC Numbers 3200-3299, 3400-3499, 3500-3599

Les références de RFC se terminant en 99 identifient le sommaire des 99 derniers documents publiés. La publication ce mois-ci des **RFC 3299**, **RFC 3499**, **RFC 3599** rattrape enfin le retard accumulé depuis plusieurs années puisque le dernier sommaire, le **RFC 3199** publié en février dernier, s'arrêtait au **RFC 3198** datant lui de novembre 2001 !

Nous proposons ci-après une liste récapitulative des RFC ayant trait au domaine de la sécurité.

RFC 3299 30 pages RFC publiés entre Décembre 2001 et Septembre 2002

3206	02/2002	The SYS and AUTH POP Response Codes
3207	02/2002	SMTP Service Extension for Secure SMTP over Transport Layer Security
3211	12/2001	Password-based Encryption for CMS
3217	12/2001	Triple-DES and RC2 Key Wrapping
3218	01/2002	Preventing the Million Message Attack on Cryptographic Message Syntax
3225	12/2001	Indicating Resolver Support of DNSSEC
3226	12/2001	DNSSEC and IPv6 A6 aware server/resolver message size requirements
3227	02/2002	Guidelines for Evidence Collection and Archiving
3230	01/2002	Instance Digests in HTTP
3235	01/2002	Network Address Translator (NAT)-Friendly Application Design Guidelines
3244	02/2002	Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols
3268	06/2002	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
3274	06/2002	Compressed Data Content Type for Cryptographic Message Syntax (CMS)
3278	04/2002	Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)
3279	04/2002	Algorithms and Identifiers for the Internet X.509 PKI Certificate and CRL Profile
3280	04/2002	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
3281	04/2002	An Internet Attribute Certificate Profile for Authorization

RFC 3499 38 pages RFC publiés entre Octobre 2002 et Mars 2003

3439	12/2002	Some Internet Architectural Guidelines and Philosophy
3447	02/2003	Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
3456	01/2003	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
3457	01/2003	Requirements for IPsec Remote Access Scenarios
3489	03/2003	STUN: Simple Traversal of User Datagram Protocol Through Network Address Translators

RFC 3599 34 pages RFC publiés entre Avril 2002 et Octobre 2003

3511	04/2003	Benchmarking Methodology for Firewall Performance
3519	05/2003	Mobile IP Traversal of Network Address Translation (NAT) Devices
3525	06/2003	Gateway Control Protocol Version 1
3526	05/2003	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
3537	05/2003	Wrapping a HMAC key with a Triple-DES Key or an Advanced Encryption Standard (AES) Key
3538	06/2003	Secure Electronic Transaction (SET) Supplement for the v1.0 Internet Open Trading Protocol
3539	06/2003	Authentication, Authorization and Accounting (AAA) Transport Profile
3546	06/2003	Transport Layer Security (TLS) Extensions
3552	07/2003	Guidelines for Writing RFC Text on Security Considerations
3554	07/2003	On the Use of Stream Control Transmission Protocol (SCTP) with IPsec
3560	07/2003	Use of the RSAES-OAEP Key Transport Algorithm in the Cryptographic Message Syntax (CMS)
3562	07/2003	Key Management Considerations for the TCP MD5 Signature Option
3565	07/2003	Use of AES Encryption Algorithm in Cryptographic Message Syntax (CMS)
3566	09/2003	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
3567	07/2003	Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
3575	07/2003	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)
3576	07/2003	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
3579	09/2003	RADIUS Support For Extensible Authentication Protocol (EAP)
3580	09/2003	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
3585	08/2003	IPsec Configuration Policy Information Model
3586	08/2003	IP Security Policy (IPSP) Requirements
3594	09/2003	PacketCable Security Ticket Control Sub-Option for the DHCP CCC Option

Seul le sommaire concernant la série 33xx est encore manquant, mais gageons qu'il ne devrait pas tarder à être publié.

<ftp://ftp.rfc-editor.org/in-notes/rfc3299.txt>

- RFC 3299

<ftp://ftp.rfc-editor.org/in-notes/rfc3499.txt>

- RFC 3499

<ftp://ftp.rfc-editor.org/in-notes/rfc3599.txt>

- RFC 3599

LES DRAFTS

DRAFT-IETF-PKIX-LOGOTYPES

Internet X.509 Public Key Infrastructure: Logotypes in X.509 certificates

L'IETF a approuvé dernièrement le passage du document de travail intitulé '**Internet X.509 Public Key Infrastructure: Logotypes in X.509 certificates**' à l'état de proposition de standard.

Ce document spécifie une nouvelle extension permettant de référencer un logo, ou plus précisément d'indiquer la localisation des données numériques représentatives d'une image visuelle ou sonore associée au détenteur du certificat ou à son organisation d'appartenance.

L'idée ici développée n'est pas de stocker ces données dans le certificat, ce qui serait déraisonnable notamment sur le plan du volume de données devant être stocké, mais plus simplement d'enregistrer le chemin d'accès à ces données sous la forme d'une URI, l'intégrité du logo étant vérifiée par le biais d'une somme cryptographique stockée dans le certificat.

Pour éviter toute ambiguïté, la signification du logo sera explicitement désignée par un attribut permettant d'encoder le niveau de rattachement de celui-ci :

- Logo rattaché à une communauté d'intérêt, un service, une marque,
- Logo rattaché à l'organisation identifiée dans le champ '**Issuer**' du certificat,
- Logo rattaché à l'organisation identifiée dans le champ '**Subject**' du certificat,
- Logo dont la signification n'est pas explicitement spécifiée.

La proposition précise que le support du format image est mandataire, le support du format audio étant optionnel. L'image devra avoir une taille allant de 60x45 à 200x150 pixels. Dans le cas du format audio, la durée de l'enregistrement devra être comprise entre 1 et 30 secondes.

L'adoption de ce standard devrait permettre d'humaniser la notion de certificat **X-509** en lui associant un visuel directement et aisément interprétable par l'être humain. Bien entendu, la fonctionnalité proposée suppose que les éléments externes non contenus dans le certificat, à savoir, la localisation du logo et sa constitution, soient invariables.

<ftp://ftp.nordu.net/internet-drafts/draft-ietf-pkix-logotypes-13.txt>

ALERTES ET ATTAQUES

ALERTES

GUIDE DE LECTURE

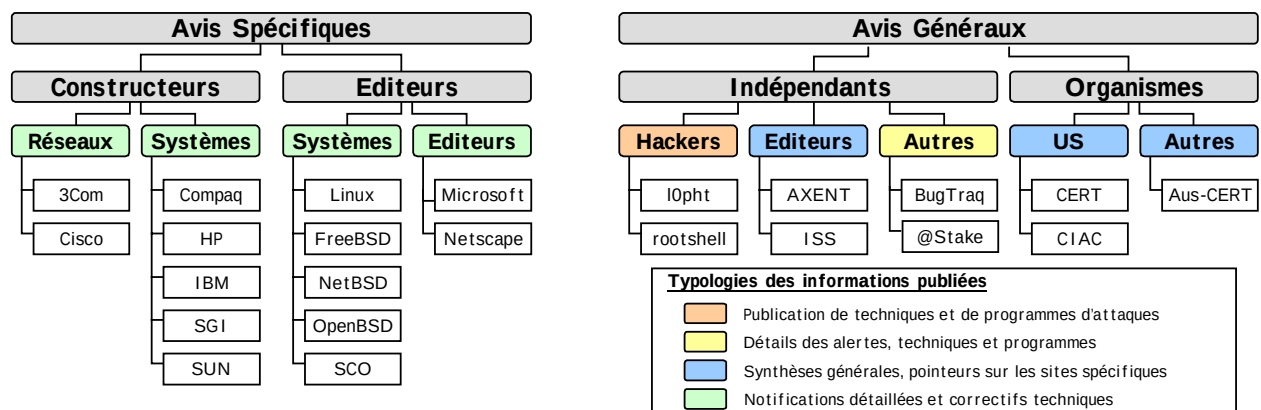
La lecture des avis publiés par les différents organismes de surveillance ou par les constructeurs n'est pas toujours aisée. En effet, les informations publiées peuvent être non seulement redondantes mais aussi transmises avec un retard conséquent par certains organismes. Dès lors, deux alternatives de mise en forme de ces informations peuvent être envisagées :

Publier une synthèse des avis transmis durant la période de veille, en classant ceux-ci en fonction de l'origine de l'avis,

Publier une synthèse des avis transmis en classant ceux-ci en fonction des cibles.

La seconde alternative, pour séduisante quelle soit, ne peut être raisonnablement mise en œuvre étant donné l'actuelle diversité des systèmes impactés. En conséquence, nous nous proposons de maintenir une synthèse des avis classée par organisme émetteur de l'avis.

Afin de faciliter la lecture de ceux-ci, nous proposons un guide de lecture sous la forme d'un synoptique résumant les caractéristiques de chacune des sources d'information ainsi que les relations existant entre ces sources. Seules les organismes, constructeurs ou éditeurs, disposant d'un service de notification officiel et publiquement accessible sont représentés.

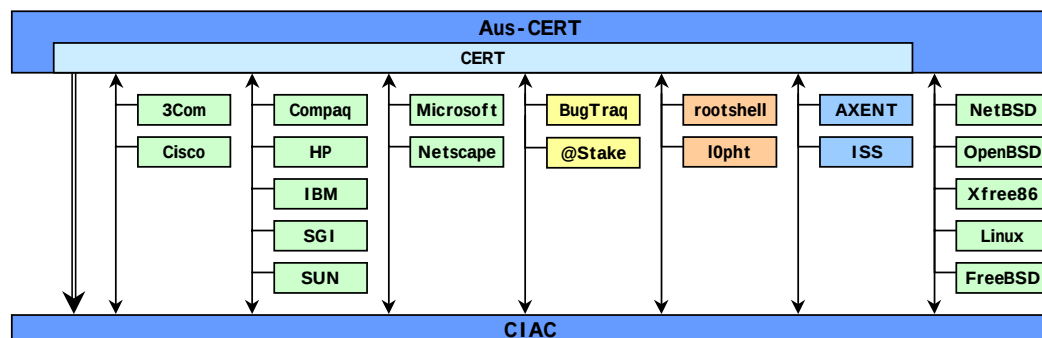


L'analyse des avis peut être ainsi menée selon les trois stratégies suivantes :

Recherche d'informations générales et de tendances : Lecture des avis du CERT et du CIAC

Maintenance des systèmes : Lecture des avis constructeurs associés

Compréhension et anticipation des menaces : Lecture des avis des groupes indépendants



FORMAT DE LA PRESENTATION

Les alertes et informations sont présentées classées par sources puis par niveau de gravité sous la forme de tableaux récapitulatifs constitués comme suit :

Présentation des Alertes

EDITEUR

TITRE		
Description sommaire		
Gravité	Date	Informations concernant la plate-forme impactée
Correction		Produit visé par la vulnérabilité Description rapide de la source du problème
Référence		URL pointant sur la source la plus pertinente
Référence(s) CVE si définie(s)		

Présentation des Informations

SOURCE

TITRE	
Description sommaire	
URL pointant sur la source d'information	
Référence(s) CVE si définie(s)	

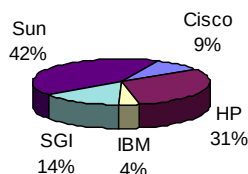
SYNTHESE MENSUELLE

Le tableau suivant propose un récapitulatif du nombre d'avis publiés pour la période courante, l'année en cours et l'année précédente. Ces informations sont mises à jour à la fin de chaque période de veille. L'attention du lecteur est attirée sur le fait que certains avis sont repris et rediffusés par les différents organismes. Ces chiffres ne sont donc représentatifs qu'en terme de tendance et d'évolution.

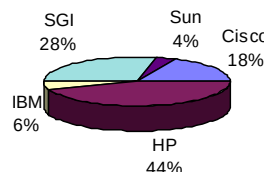
Période du **28/11/2003** au **29/12/2003**

	Période	Cumul	
		2003	2002
Organisme	14	195	165
CERT-CA	0	28	36
CERT-IN	0	4	7
CIAC	14	163	122
Constructeurs	22	305	220
Cisco	5	26	39
HP	2	95	99
IBM	1	12	13
SGI	4	44	61
Sun	10	128	8
Editeurs	3	88	127
Macromedia	2	8	13
Microsoft	0	51	72
Netscape	0	0	2
Sco	1	29	40
Unix libres	20	464	349
Linux RedHat	7	129	102
Linux Debian	2	192	120
Linux Mandr.	10	116	85
FreeBSD	1	27	42
Autres	1	49	44
@Stake	0	28	9
eEye	0	9	13
X-Force	1	12	22

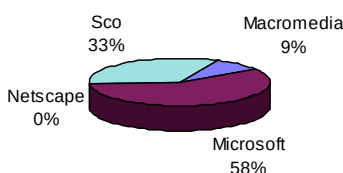
Cumul 2003- Constructeurs



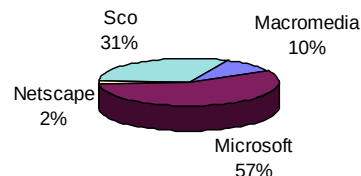
Cumul 2002 - Constructeurs



Cumul 2003 - Editeurs



Cumul 2002 - Editeurs



ALERTES DETAILLEES

AVIS OFFICIELS

Les tables suivantes présentent une synthèse des principales alertes de sécurité émises par un organisme fiable, par l'éditeur du produit ou par le constructeur de l'équipement. Ces informations peuvent être considérées comme fiables et authentifiées. En conséquence, les correctifs proposés, s'il y en a, doivent immédiatement être appliqués.

APPLE

Multiples vulnérabilités dans MacOS X

De multiples vulnérabilités affectent Mac OS X version 10.3.2.

Forte	19/12	Apple Mac OS X version 10.3.2
Correctif existant	Binaires, système	Multiples vulnérabilités
AusCERT		http://www.uscert.org.au/render.html?it=3704&cid=1
CAN-2003-1007, CAN-2003-1005, CAN-2003-1006, CAN-2003-1009, CAN-2003-0792, CAN-2003-1010, CAN-2003-0962, CAN-2003-1008, CAN-2003-1011		

BIND

Compromission du cache DNS dans BIND

BIND 8 est vulnérable à des attaques conduisant à la compromission du cache DNS.

Forte	26/11	ISC BIND versions inférieures à 8.3.7 et 8.4.3
Correctif existant	BIND	Enregistrement non autorisé de données dans le cache
ISC		http://www.isc.org/products/BIND/bind8.html
CAN-2003-0914		

CA

Multiples vulnérabilités dans Unicenter Remote Control

De multiples vulnérabilités dans les produits Unicenter Remote Control et ControlIT peuvent conduire à l'acquisition de droits privilégiés et à un déni de service.

Forte	11/12	1 - CA Unicenter Remote Control 5.2, Option 5.0, Option 5.1, Control IT Enterprise 5.0, 5.1, Control IT Ad 5.0 2, 3 - Computer Associates Unicenter Remote Control 6.0
Correctif existant	'Remote Control' et 'ControlIT'	Non disponible
CA		http://support.ca.com/techbases/rp/urc6x-secnote.html
CA		http://support.ca.com/techbases/rp/urc5x-secnote.html

CISCO

Débordement de buffer dans ACNS

Un débordement de buffer dans ACNS peut autoriser un utilisateur distant à exécuter du code arbitraire.

Forte	10/12	Cisco ACNS versions inférieures à 4.2.11 ou 5.0.5
Palliatif proposé	'ACNS'	Débordement de buffer
Cisco 47184		http://www.cisco.com/warp/public/707/cisco-sa-20031210-ACNS-auth.shtml

Exposition des clés WEP statiques

Une vulnérabilité dans Cisco Aironet permet d'exposer les clés WEP statiques.

Forte	02/12	Cisco Aironet séries 1100, 1200 et 1400 avec Cisco IOS 12.2(8)JA, 12.2(11)JA et 12.2(11)JA1
Palliatif proposé	Cisco IOS	Mauvaise gestion des traps SNMP
Cisco 46468		http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.shtml

Multiples vulnérabilités sur Cisco Unity

Les récentes installations de Cisco Unity sur serveurs IBM possèdent des comptes utilisateur et des adresses IP positionnés par défaut qu'il est nécessaire de supprimer ou de désactiver.

Forte	11/12	Cisco Unity sur serveurs IBM (cf. liste 'part numbers')
Palliatif proposé	Cisco Unity	1 - Existence d'un compte utilisateur 2, 3 - Existence d'adresses IP positionnées par défaut
Cisco 47186		http://www.cisco.com/warp/public/707/cisco-sa-20031210-unity.shtml

Déni de service dans les pare-feu Pix

Deux vulnérabilités conduisant à un déni de service affectent les pare-feu Cisco Pix.

Forte	15/12	1 - Cisco PIX firewall version 6.3.1, 6.2.2 et inférieures, 6.1.4 et inférieures et 5.x.x et inférieures 2 - Cisco PIX firewall version 6.2.3 et inférieures
Correctif existant	1 - Traitement paquet SNMPv3 2 - Client VPN	1 - Mauvais traitement des paquets 2 - Conflit d'accès sur les sessions
Cisco 47284		http://www.cisco.com/warp/public/707/cisco-sa-20031215-pix.shtml

Vulnérabilités dans FWSM		
<i>Deux vulnérabilités dans Cisco Firewall Services Module peuvent entraîner un déni de service des équipements.</i>		
Forte	15/12	Cisco FWSM version 1.1.2 et inférieure pour Catalyst séries 6500 et 7600
Palliatif proposé	Firewall Services Module	1 - Débordement de buffer 2 - Mauvaise gestion des requêtes SNMPv3
Cisco 47288	http://www.cisco.com/warp/public/707/cisco-sa-20031215-fwsml.html	

CVS

Vulnérabilité dans CVS		
<i>Une vulnérabilité dans CVS peut autoriser un utilisateur distant à créer des fichiers et des répertoires de manière arbitraire.</i>		
Forte	09/12	CVS version 1.11.9 et inférieure
Correctif existant	'cvs'	Mauvaise gestion des requêtes
Security Tracker	http://www.securitytracker.com/alerts/2003/Dec/1008420.html	
CVS	http://ccvs.cvshome.org/servlets/NewsItemView?newsID=84&JServSessionIdservlets=8u3x1myav1	

ETHEREAL

Déni de service dans Ethereal		
<i>Deux vulnérabilités dans Ethereal peuvent conduire à un déni de service.</i>		
Forte	03/11	Ethereal 0.9.16
Correctif existant	Dissecteurs Q.931 et SMB	Déférencement de pointeur NULL
Ethereal 00012	http://www.ethereal.com/appnotes/enpa-sa-00012.html	

GnuPG

Révélation de la clé privée ElGamal sign+encrypt		
<i>Une faille dans GnuPG autorise un utilisateur à prendre connaissance de la clé privée ElGamal sign+encrypt de son correspondant.</i>		
Forte	27/11	GnuPG version 1.0.2 et supérieures lors de l'utilisation de clés ElGamal sign+encrypt (type 20)
Aucun correctif	Génération de clés type 20	Utilisation d'un facteur commun pour le chiffrement et la signature
GnuPG	http://lists.gnupg.org/pipermail/gnupg-announce/2003q4/000276.html	

HP

Création non sécurisée de fichiers dans 'shar'		
<i>Une vulnérabilité dans l'utilitaire 'shar' peut conduire un utilisateur local à acquérir des droits privilégiés.</i>		
Forte	01/12	HP HP-UX versions B.11.00, B.11.04 et B.11.11
Correctif existant	'shar'	Création de fichiers non sécurisée
HPSBUX0312-304	http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0312-304	

Dégradation des performances réseau sur HP ProCurve		
<i>Les commutateurs HP ProCurve sont vulnérables à des attaques par déni de service.</i>		
Moyenne	24/11	HP ProCurve Switch 5304XL, 5348XL, 5372XL et 5308XL
Correctif existant	Trafic RPC généré par les vers Blaster et Welchia	Dégradation des performances réseau
HPSBMI0311-006	http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBMI0311-006	

IBM

Multiples vulnérabilités dans les commandes AIX		
<i>Des vulnérabilités dans les commandes 'enq' et 'diag' peuvent autoriser un utilisateur local à acquérir des droits privilégiés.</i>		
Forte	17/12	IBM AIX 4.3, 5.1 et 5.2
Correctif existant	1 - Commande 'enq' 2 - Commande 'diag'	1 - Mauvaise gestion de chaînes de caractères 2 - Non disponible
OAR-E01-03:1600	http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1600.1	
OAR-E01-03:1599	http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1599.1	
CAN-2003-1018		

Création de répertoires non sécurisée dans DB2		
<i>La base de données IBM DB2 est vulnérable à des créations non sécurisées de répertoires.</i>		
Moyenne	18/12	IBM DB2 Universal Database 7.x pour AIX
Correctif existant	'db2'	Création non sécurisée de répertoires
IBM IY44841	http://www-306.ibm.com/cgi-bin/db2www/data/db2/.../aparlib.d2w/display_apar_details?aparno=IY44841	

KERIO

Balayage des ports TCP sur KPF

Une vulnérabilité dans Kerio Personal Firewall autorise un utilisateur distant contourner le pare-feu.

Forte	21/12	Kerio Personal Firewall version 4.0.9 et inférieures
Correctif existant	KPF (Kerio Personal Firewall)	Contournement du pare-feu
Kerio	http://www.kerio.com/kpf_releasehistory.html	

LINUX

Débordement de buffer distant dans 'rsync'

Un débordement de buffer exploitable à distance dans 'rsync' permet d'exécuter un code arbitraire sur les serveurs vulnérables.

Critique	05/12	'rsync' version 2.5.6 et inférieures
Palliatif proposé	Serveurs 'rsync'	Débordement de buffer
RHSA-03:399-06	https://rhn.redhat.com/errata/RHSA-2003-399.html	
Bugtraq	http://www.securityfocus.com/advisories/6140	
SuSE-SA:03:050	http://www.suse.de/de/security/2003_050_rsync.html	
Projet 'rsync'	http://samba.anu.edu.au/rsync/	
FEDORA-03-030	http://www.redhat.com/archives/fedora-announce-list/2003-December/msg00002.html	
OpenBSD	http://www.auscert.org.au/render.html?it=3669&cid=1	
DSA-404-1	http://lists.debian.org/debian-security-announce/debian-security-announce-2003/msg00213.html	
RHSA-03:398-07	https://rhn.redhat.com/errata/RHSA-2003-398.html	
CAN-2003-0962		

Débordement de buffer dans le noyau Linux

Un débordement de buffer dans le noyau Linux peut autoriser un utilisateur à acquérir des droits privilégiés sur le système.

Critique	01/12	Linux noyau versions 2.4.22 et inférieures
Correctif existant	Fonction 'do_brk'	Débordement de buffer
DSA-403-1	http://www.debian.org/security/2003/dsa-403	
RHSA-03:392-05	https://rhn.redhat.com/errata/RHSA-2003-392.html	
iSEC Security	http://isec.pl/vulnerabilities/isec-0012-do_brk.txt	
CAN-2003-0961		

LINUX SuSE

Deux vulnérabilités dans 'gpg' (gnupg)

Deux vulnérabilités affectent le packaging 'gpg' (gnupg) pour SuSE.

Forte	03/12	SuSE Linux versions 7.3, 8.0, 8.1, 8.2, 9.0 et serveurs
Correctif existant	1 - Génération de clés type 20 2 - Code client	1 - Facteur commun dans le chiffrement et la signature 2 - Mauvais formatage de chaîne de caractères
S-Quad. 03-12-03	http://www.s-quadra.com/advisories/Adv-20031203.txt	
SuSE-SA:03:048	http://www.suse.de/de/security/2003_048_gpg.html	
CAN-2003-0971		

MACROMEDIA

Exposition d'informations via Flash Player

Une faille dans Internet Explorer et Opera permet d'obtenir des informations via le lecteur Flash.

Forte	16/12	Macromedia Flash Player versions inférieures à 7,0,19,0
Correctif existant	Lecteur Flash	Exploitation d'une faille dans Internet Explorer et Opera
MPSB03-08	http://www.macromedia.com/devnet/security/security_zone/mpsb03-08.html	

MODPYTHON

Déni de service dans 'mod_python'

Une vulnérabilité dans 'mod_python' peut provoquer un déni de service du serveur Apache.

Forte	28/11	'mod_python' versions inférieures à 2.7.9 (Apache V 1.3) et versions inférieures à 3.0.4 (Apache V 2.0)
Correctif existant	'mod_python'	Mauvaise gestion des requêtes
Security Tracker	http://www.securitytracker.com/alerts/2003/Nov/1008335.html	
Modpython	http://www.modpython.org/pipermail/mod_python/2003-November/004006.html	

NOVELL

Contournement des restrictions d'accès dans NFS

Une vulnérabilité dans NetWare 6.5 peut permettre à un utilisateur malveillant de contourner les restrictions d'accès à des partages NFS.

Forte	04/12	Novell NetWare 6.5
Correctif existant	'XNFS.NLM'	Mauvaise gestion des fichiers de configuration
Novell 10089375	http://support.novell.com/cgi-bin/tidfinder/10089375	

OPERA

Vulnérabilité dans le navigateur Opera

Une vulnérabilité dans le navigateur Opera peut autoriser un utilisateur distant à écraser ou supprimer des fichiers arbitraires.

Forte	12/12	Opera version 7.22 et inférieure pour plateforme Windows
Correctif existant	'opera'	Mauvaise gestion des caractères
Operash	http://opera.rainyblue.org/modules/cjaycontent/index.php?id=16	

Vulnérabilités dans Opera

Deux vulnérabilités affectent le navigateur Opera.

Forte	23/12	1 - Opera versions 7 à 7.22, 2 - Opera versions 6.06 à 7.22
Correctif existant	Navigateur Opera	1 - Mauvaise gestion des noms de fichiers temporaires 2 - Non échappement des caractères de contrôle d'une URL
Operash	http://opera.rainyblue.org/modules/cjaycontent/index.php?id=16	
Bugtraq	http://www.securityfocus.com/archive/1/348275	

SOAP

Déni de service dans les serveurs SOAP

Un mauvais traitement des requêtes par les serveurs SOAP permet de provoquer un déni de service.

Forte	09/12	IBM WebSphere versions 5.0.0, 5.0.1, 5.0.2 et 5.0.2.1 Microsoft ASP.NET Web Services (.NET framework 1.0 et 1.1) Macromedia JRun 4.0 (toutes éditions), ColdFusion MX 6.0, 6.1 et MX 6.0, 6.1 J2EE (toutes éditions)
Correctif existant	Analyseur XML Crimson	Mauvais traitement des requêtes
Microsoft 832878	http://support.microsoft.com/default.aspx?kbid=832878	
MPSB03-07	http://www.macromedia.com/devnet/security/security_zone/mpsb03-07.html	
IBM PQ81278	http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q=PQ81278&uid=swg24005943	
Bugtraq	http://www.securityfocus.com/archive/1/346973	

SUN

Vulnérabilités OpenSSL sur Sun Grid Engine

Sun Grid Engine est vulnérables aux failles OpenSSL récemment découvertes.

Critique	22/12	Sun Grid Engine 5.3 (Sparc 32 et 64 bits, Intel) incluant le format de paquetage NON-Solaris pour Sun Linux	
Correctif existant	OpenSSL	Vulnérabilité aux failles OpenSSL	
Sun 57444	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57444		
CAN-2003-0543, CAN-2003-0544, CAN-2003-0545			

Démarrage d'exécutables à distance via J2EE

Une vulnérabilité dans le composant Pointbase permet de démarrer un exécutable quelconque via une requête SQL.

Forte	16/12	Sun J2EE/RI 1.4 (pour Windows) avec composant Pointbase 4.6
Palliatif proposé	J2EE/RI et Pointbase 4.6	Mauvais gestion des requêtes SQL
Security Tracker	http://www.securitytracker.com/alerts/2003/Dec/1008491.html	

Accès non autorisé aux fichiers via PC Netlink

Une vulnérabilité dans PC Netlink permet d'accéder à des fichiers ou des répertoires protégés par ACLs.

Forte	01/12	Sun PC Netlink 1.x (Sparc et Intel)
Correctif existant	Processus de sauvegarde	Perte des informations concernant les ACLs
Sun 27807	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/27807	

Création non sécurisée de fichiers dans 'Xsun'

Les systèmes Solaris utilisant 'Xsun' sont vulnérables lors de la création de fichiers temporaires.

Forte	02/12	Sun Solaris 2.6 à 9 (Sparc et Intel)
Correctif existant	Serveur graphique 'Xsun'	Création de fichiers non sécurisée
Sun 57419	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57419	

Déni de service dans Sun ONE Web Server

Le serveur web Sun ONE est sensible à des attaques par déni de service.

Forte	02/12	Sun ONE/iPlanet Web Server 4.1 SP12 et inférieurs (Windows), Web Server 6.0 SP5 et inférieurs (Windows)
Correctif existant	Serveurs web Sun ONE/iPlanet	Non disponible
Sun 57423	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57423	

Débordement de buffer dans 'dtprintinfo'

Une vulnérabilité dans 'dtprintinfo' permet d'exécuter un code arbitraire sous les droits 'root'.

Forte	04/12	Sun Solaris 2.6 à 9 (Sparc et Intel)
Correctif existant	'dtprintinfo'	Débordement de buffer
Sun 57441	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57441	

Création non sécurisée de fichiers dans 'ed'			
Une vulnérabilité dans l'éditeur de texte 'ed' peut conduire un utilisateur local à acquérir des droits privilégiés.			
Forte	10/12	Sun Solaris 2.6, 7 et 8 (Sparc et x86)	
Correctif existant	'ed'	Création de fichiers non sécurisée	
Sun 57443	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57443		
Acquisition de droits dans Sun Solaris			
De multiples vulnérabilités dans les services d'impression de Sun Solaris peuvent conduire à l'acquisition de droits privilégiés.			
Forte	12/12	Sun Solaris 2.6 à 9 (Sparc et x86)	
Correctif existant	'lpstat' et bibliothèque 'libprint'	Non disponible	
Sun 57451	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57451		
Vulnérabilité dans 'tcsh'			
Une vulnérabilité non documentée dans l'interpréteur de commande 'tcsh' peut autoriser un utilisateur local à acquérir des droits privilégiés et à la manipulation de fichiers arbitraires.			
Forte	22/12	Sun Solaris 8 (Sparc et x86)	
Correctif existant	Interpréteur 'tcsh'	Non disponible	
Sun 57455	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57455		
Cross-Site Scripting dans Sun ONE Web Server 6.1			
Une vulnérabilité de type Cross-Site Scripting affecte les serveurs web Sun ONE.			
Moyenne	27/11	Sun ONE Web Server 6.1	
Aucun correctif	Interface d'administration	Cross-Site Scripting	
Dr. Insane	http://members.lycos.co.uk/r34ct/main/SUN_WEB_SERVER.6.1/SUN-web-server.6.1-CSS.txt		
Déni de service dans Sun Cluster			
Un conflit d'accès au port TCP peut conduire à un déni de service sur Sun Cluster.			
Moyenne	25/11	Sun Cluster 2.2 pour Solaris 2.6, 7 et 8 (Sparc), Sun Cluster 3.0 et 3.1 pour Solaris 8 et 9 (Sparc)	
Aucun correctif	Sun Cluster	Conflit d'accès au port TCP	
Sun 57428	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57428		
Dégradation de performances sur Sun Fire B1600			
L'envoi de paquets ARP à destination du port d'administration de Sun Fire B1600 peut conduire à la dégradation des performances réseau.			
Moyenne	24/11	Sun Fire B1600 Blade System Chassis	
Correctif existant	Port d'administration	Perte de paquets	
Sun 57430	http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57430		

ALERTES NON CONFIRMÉES

Les alertes présentées dans les tables de synthèse suivantes ont été publiées dans diverses listes d'information mais n'ont pas encore fait l'objet d'une annonce ou d'un correctif de la part de l'éditeur. Ces alertes nécessitent la mise en place d'un processus de suivi et d'observation.

APPLE

Déni de service dans Appleshare IP			
Une vulnérabilité non documentée dans le serveur FTP Appleshare IP permet à un utilisateur distant authentifié de provoquer un déni de service.			
Forte	05/12	Apple Appleshare IP version 6.3.1 et inférieures	
Correctif existant	Serveur FTP Appleshare IP	Non disponible	
Bugtraq	http://www.securityfocus.com/archive/1/346612		
Débordement de buffer dans 'cd9660.util'			
Une vulnérabilité affecte l'utilitaire 'cd9660.util' livré avec Mac OS X.			
Forte	15/12	Apple Mac OS X	
Aucun correctif	Utilitaire 'cd9660.util'	Débordement de buffer local	
Security Tracker	http://www.securitytracker.com/alerts/2003/Dec/1008484.html		
Vulnérabilité dans Mac OS X			
Une vulnérabilité dans Mac OS X peut conduire à introduire un serveur d'authentification malicieux dans la liste des sources d'authentification du système.			
Forte	26/11	Apple Mac OS X 10.2 à 10.3.1 Il est possible que les versions inférieurs de Mac OS X soient vulnérables.	
Aucun correctif	Mac OS X	Erreur de conception	
SecurityTracker	http://www.securitytracker.com/alerts/2003/Nov/1008307.html		
William Carrel	http://www.carrel.org/dhcp-vuln.html		

APPLIED WATCH

Vulnérabilités dans Applied Watch Command Center

De nombreuses vulnérabilités affectent Applied Watch Command Center.

Forte	27/11	Applied Watch Server versions inférieures à 1.4.5 Applied Watch Command Center (Linux, Solaris, OpenBSD, HP-UX, Tru64 et Windows NT)	
Palliatif proposé		Applied Watch Console et Node	Multiples vulnérabilités
Applied Watch		http://www.bugtraq.org/advisories/_BSSADV-0000-VENDOR_RESPONSE.txt	
BtraqSS 0000		http://www.bugtraq.org/advisories/_BSSADV-0000.txt	
CAN-2003-0970, CAN-2003-0971			

ARC

Cross-Site Scripting dans l'outil d'audit SARA

L'outil d'audit SARA est vulnérable à des attaques par Cross-Site Scripting.

Forte	17/12	SARA versions 4.2.6 et 4.2.7 Des versions inférieures sont probablement vulnérables.
Correctif existant	SARA	Cross-Site Scripting
Bugtraq	http://www.securityfocus.com/archive/1/347846	

CYBERGUARD

Exécution de Script arbitraire via le proxy HTTP

Une faille de type Cross Site Scripting permet l'exécution de script arbitraire via le proxy HTTP de CyberGuard.

Forte	22/12	CyberGuard proxy/firewall version 5.1
Palliatif proposé	Proxy HTTP	Cross Site Scripting
Security Tracker	http://www.securitytracker.com/alerts/2003/Dec/1008526.html	

DAMEWARE

Débordement de buffer distant dans DameWare

Un débordement de buffer exploitable à distance affecte DameWare.

Forte	15/12	DameWare version 3.72 et inférieures
Correctif existant	'DWRCS.exe'	Débordement de buffer distant
Sh0dan	http://sh0dan.org/files/dwmrcs372.txt	

FreeRADIUS

Débordement de buffer dans FreeRADIUS

Le module expérimental 'rlm_smb' de FreeRADIUS est sensible à un débordement de buffer pouvant conduire un utilisateur à acquérir des droits privilégiés sur le système ou à provoquer un déni de service.

Forte	26/11	FreeRADIUS version 0.9.3 et inférieures
Correctif existant	Module 'rlm_smb'	Débordement de buffer
S-Quadra	http://www.securityfocus.com/archive/1/345692	

GNU

Débordement de buffer dans 'screen'

Un débordement de buffer affecte l'application GNU 'screen'.

Moyenne	28/11	GNU screen versions 4.0.1, 3.9.15 et inférieures
Aucun correctif	'ansi.c' via l'application 'screen'	débordement de buffer
Security Tracker	http://www.securitytracker.com/alerts/2003/Nov/1008321.html	

IBM

Cross-Site Scripting dans Tivoli Directory Server

Une faille de type Cross-Site Scripting permet d'exécuter du script arbitraire sur IBM Directory Server.

Moyenne	02/12	IBM Tivoli Directory Server version 4.1 (sur Windows)
Aucun correctif	Programme 'ldacgi.exe'	Cross-Site Scripting
Bugtraq	http://www.securityfocus.com/archive/1/346181	

IKE

Vulnérabilités dans les implémentations IKE

Plusieurs implémentations IKE sont sensibles à deux vulnérabilités.

Forte	12/12	1, 2 - Certicom Movian VPN, Cisco client VPN 3002 Hardware et client VPN 5000, VPN Client 2.0 à 4.0.2 C 2 - FreeS/WAN versions 1.9 à 1.9.6, Microsoft Windows 2000 et XP
Aucun correctif	Implémentations IKE	Mauvais processus de vérification des certificats
SF 9209	http://www.securityfocus.com/bid/9209	
Bugtraq	http://www.securityfocus.com/archive/1/347351	
SF 9208	http://www.securityfocus.com/bid/9208	

IPSWITCH

Déni de service dans les serveurs FTP 'WS_FTP'

Un déni de service affecte à distance les serveurs FTP 'WS_FTP'.

Forte	18/12	Ipswitch WS_FTP Server version 4.02	
Aucun correctif		Serveur FTP 'WS_FTP'	Mauvaise gestion des commandes
Dr insane		http://members.lycos.co.uk/r34ct/main/WS-ftp_4.0.2/WSFTP.txt	

L-Soft

Cross-Site Scripting dans LISTSERV

Le serveur de liste LISTSERV est sensible à des attaques de type Cross-Site Scripting (XSS).

Forte	27/12	L-Soft LISTSERV 1.x	
Correctif existant		Composant 'wa.exe'	Cross-Site Scripting
Security Tracker		http://www.securitytracker.com/alerts/2003/Dec/1008551.html	

LFTP

Débordements de buffer dans LFTP

Le client ftp LFTP est sensible à des débordements de buffer pouvant conduire à l'exécution de code arbitraire.

Forte	14/12	LFTP versions inférieures à 2.6.10	
Correctif existant		Deux fonctions spécifiques	Débordement de buffer
Security Tracker		http://www.securitytracker.com/alerts/2003/Dec/1008463.html	
CAN-2003-0963			

LINKSYS

Déni de service dans le produit Linksys WRT54G

Le firmware 1.42.3 du produit Linksys WRT54G est sensible à un déni de service.

Forte	03/12	Linksys Wireless-G Broadband Router WRT54G v1.0 (Firmware 1.42.3)	
Aucun correctif		Firmware	Mauvaise gestion des requêtes HTTP
Bugtraq		http://www.securityfocus.com/archive/1/346399	

MACROMEDIA

Cross-Site Scripting dans Macromedia JRun 4

Une faille de type Cross-Site Scripting permet d'exécuter un script arbitraire via l'interface administrative de JRun.

Forte	27/11	Macromedia JRun 4 (build 61650) toutes plate-formes	
Aucun correctif		Interface administrative JRun	Cross-Site Scripting
Dr. Insane		http://members.lycos.co.uk/r34ct/main/Macromedia_JRUN/Macromedia_jrun_4.0.txt	

MICROSOFT

Multiples vulnérabilités dans Internet Explorer

De multiples vulnérabilités affectent le navigateur Internet Explorer et peuvent compromettre le système.

Critique	25/11	Microsoft Internet Explorer 6 SP1 et inférieurs	
Aucun correctif		Internet Explorer	Multiples vulnérabilités
Bugtraq		http://www.securityfocus.com/archive/1/345619	
Liu Die Yu		http://die.leox.com/DirSvc/security/originality/microsoft_ie/index.html	
Bugtraq		http://www.securityfocus.com/archive/1/345614	

Analyse des nouveaux vecteurs d'attaque sur DCE RPC

De nouveaux vecteurs d'attaque exploitant les vulnérabilités DCE RPC ont été découverts.

Forte	10/12	Microsoft Windows 2000 et XP avec les services RPC activés	
Correctif existant		Services DCE RPC	Découverte de nouveaux vecteurs d'attaque
CORE-03-12-05		http://www.coresecurity.com/common/showdoc.php?idx=393&idxsection=10	
CAN-2003-0003, CAN-2003-0352, CAN-2003-0717, CAN-2003-0812			

Usurpation du domaine visité via Internet Explorer

Une faille dans Internet Explorer permet l'usurpation du domaine visité.

Forte	09/12	Microsoft Internet Explorer version 6 et inférieures	
Aucun correctif		Internet Explorer	Non échappement des caractères de contrôle d'une URL
Zap The Dingbat		http://zapheddingbat.com/security/ex01/vun1.htm	

Vulnérabilité dans IIS

Le serveur WEB IIS n'enregistre pas la requête 'TRACK' dans les journaux.

Moyenne	28/12	Microsoft Internet Information Services 5.0	Il est possible que des versions inférieures soient vulnérables
Aucun correctif		Internet Information Services	Mauvaise gestion de la commande HTTP 'TRACK'
AQ-03-02		http://www.aqtronix.com/Advisories/AQ-2003-02.txt	

Exécution de code arbitraire via Internet Explorer

Une faille dans Internet Explorer permet de contourner des messages d'alerte lors du téléchargement d'un fichier.

Moyenne	23/12	Microsoft Internet Explorer (testé sur Windows 2003)
Aucun correctif	Processus de téléchargement	Contourner des messages d'alerte
Info Hacking	http://www.infohacking.com/INFOHACKING_RESEARCH/Our_Advisories/IE/index.html	

Exposition d'informations dans Internet Explorer

Une vulnérabilité dans le navigateur Internet Explorer pour système Mac OS peut conduire à l'exposition d'informations.

Moyenne	26/12	Microsoft Internet Explorer 5.22 pour système Mac OS
Aucun correctif	'Internet Explorer'	Non respect de la norme HTTP/1.1
Security Tracker	http://www.securitytracker.com/alerts/2003/Dec/1008554.html	
SF 9295	http://www.securityfocus.com/bid/9295	

NETGEAR

Erreur de configuration dans NetGear WAB102

Une erreur de configuration sur NetGear WAB102 permet de s'authentifier sur le dispositif.

Forte	11/12	NetGear WAB102 avec firmware version 1.2.3
Aucun correctif	Point d'accès NetGear WAB102	Erreur de configuration
Security Tracker	http://www.securitytracker.com/alerts/2003/Dec/1008445.html	

OPENCA

Utilisation d'un certificat expiré ou révoqué

Une vulnérabilité dans OpenCA permet d'accepter un certificat expiré ou révoqué.

Forte	01/12	OpenCA version 0.9.1-3 et inférieures
Correctif existant	Bibliothèque 'crypto-utils.lib' Module 'OpenCA::PKCS7'	Mauvaises vérification de la chaîne de certificats
Full Disclosure	http://lists.netsys.com/pipermail/full-disclosure/2003-November/014273.html	
CAN-2003-0960		

PHP

Vulnérabilité dans le module 'mod_php'

Une vulnérabilité dans le module 'mod_php' permet de détourner le service HTTPS.

Forte	26/12	PHP versions 4.2 et 4.3 avec le module 'mod_php' sous Apache version 2.0
Aucun correctif	Module 'mod_php'	Mauvaise gestion des appels externes
Bugtraq	http://www.securityfocus.com/archive/1/348368	

SQUIRRELMAIL

Exécution de commandes arbitraires via SquirrelMail

Le passage de données spécialement construites au champ 'To:' d'un e-mail envoyé avec SquirrelMail permet d'exécuter des commandes arbitraires.

Forte	24/12	SquirrelMail (toutes plate-formes)
Aucun correctif	'gpg_encrypt.php'	Non validation des données utilisateurs
Site 'bugtraq.org'	http://www.bugtraq.org/advisories/_BSSADV-0001.txt	
CAN-2003-0990		

SYBASE

Multiplés vulnérabilités dans Sybase Anywhere 9

Sybase SQL Anywhere 9 est sensible à de multiples vulnérabilités.

Forte	10/12	Sybase SQL Anywhere 9
Correctif existant	'Adaptive Server Anywhere'	Mauvaise gestion des chaînes de caractères, Débordements de buffer
NGSSoftware	http://www.securityfocus.com/archive/1/347073	

WEBSense

Cross-Site Scripting dans Websense Enterprise

Websense Enterprise est vulnérable à des attaques par Cross-Site Scripting.

Forte	03/12	Websense Enterprise version 4.3.0 et 5.1
Aucun correctif	Websense	Cross-Site Scripting
Bugtraq	http://www.securityfocus.com/archive/1/346340	

XEROX

Exposition de données sensibles sur Document Centre

Une vulnérabilité du serveur web embarqué sur Xerox Document Centre permet d'accéder à des données sensibles.

Forte	22/12	Xerox Document Centre 470 (255ST) avec Xerox_MicroServer/Xerox11 0.19.5.509
Palliatif proposé	Serveur web embarqué	Non filtrage des URLs
Security Tracker	http://www.securitytracker.com/alerts/2003/Dec/1008523.html	

YAHOO!

Débordement de buffer distant dans Instant Messenger

Un débordement de buffer distant affecte Instant Messenger.

Forte 02/12 Yahoo! Instant Messenger version 5.6.0.1347 et inférieures

Palliatif proposé Composant ActiveX 'YAUTO.DLL' Débordement de buffer distant

Full Disclosure <http://lists.netsys.com/pipermail/full-disclosure/2003-December/014434.html>

AUTRES INFORMATIONS

REPRISES D'AVIS ET CORRECTIFS

Les vulnérabilités suivantes, déjà publiées, ont été mises à jour, reprises par un autre organisme, ou ont donné lieu à la fourniture d'un correctif :

APPLE

Correctifs pour le navigateur Safari

Apple a annoncé la disponibilité des correctifs du navigateur Safari pour Mac OS X 10.2.8 et 10.3.1. Une faille permet de récupérer les 'cookies' utilisateurs appartenant à un site tiers.

<http://www.info.apple.com/kbnum/n120282>

<http://www.info.apple.com/kbnum/n120283>

CAN-2003-0975

CERT

Complément d'informations sur la vulnérabilité BIND

Un complément d'informations a été publié par le CERT au sujet de la vulnérabilité affectant BIND et pouvant conduire à un déni de service. La liste des éditeurs vulnérables recense à ce jour les implémentations FreeBSD, Guardian Digital, HP, IBM, Immunix, ISC, NetBSD, Nixu, Sun, SuSE et Trustix. Par ailleurs, SCO est aussi vulnérable.

<http://www.kb.cert.org/vuls/id/734644>

CAN-2003-0914

CIAC

Reprise de l'avis Cisco 47284

Le CIAC a repris, sous la référence O-040, l'avis Cisco 47284 traitant de deux vulnérabilités dans les pare-feu Pix pouvant conduire à un déni de service.

<http://www.ciac.org/ciac/bulletins/o-040.shtml>

Reprise de l'avis Sun 57451

Le CIAC a repris, sous la référence O-041, l'avis Sun 57451 traitant de multiples vulnérabilités dans les services d'impression de Sun Solaris peuvent conduire un utilisateur local à acquérir les droits privilégiés 'root'.

<http://www.ciac.org/ciac/bulletins/o-041.shtml>

Reprise de l'avis Red Hat RHSA-2003:403

Le CIAC a repris, sous la référence O-041, les avis Red Hat RHSA-2003:403 et RHSA-2003:404 traitant des débordements de buffer dans le client ftp 'lftp' pouvant conduire à l'exécution de code arbitraire.

<http://www.ciac.org/ciac/bulletins/o-042.shtml>

CAN-2003-0963

Reprise de l'avis HP HPSBUX0311-302

Le CIAC a repris, sous la référence O-030, l'avis HP HPSBUX0311-302 au sujet d'un débordement de buffer dans OpenSSH pour le système HP-UX B.11.04 (VVO) avec VirtualVault A.04.60.

<http://www.ciac.org/ciac/bulletins/o-030.shtml>

CAN-2003-0693, CAN-2002-0083

Reprise de l'avis Red Hat RHSA-2003:408

Le CIAC a repris, sous la référence O-043, l'avis Red Hat RHSA-2003:408 au sujet de la disponibilité des correctifs noyaux. Ils éliminent une vulnérabilité autorisant un utilisateur local à acquérir des droits privilégiés lui permettant d'accéder aux descripteurs de fichiers restreints.

<http://www.ciac.org/ciac/bulletins/o-043.shtml>

CAN-2003-0476

Reprise de l'avis Sun 57455

Le CIAC a repris, sous la référence O-044, l'avis Sun 57455 concernant une vulnérabilité dans l'interpréteur de commande 'tcsh' pouvant autoriser un utilisateur local à acquérir des droits privilégiés et à la manipulation de fichiers arbitraires.

<http://www.ciac.org/ciac/bulletins/o-044.shtml>

Reprise de l'avis Linux
Le CIAC a repris, sous la référence O-031, l'avis Linux au sujet d'un débordement de buffer dans la fonction 'do_brk()' permettant d'acquérir les droits privilégiés 'root'.
http://ciac.llnl.gov/ciac/bulletins/o-031.shtml
CAN-2003-0961
Reprise de l'avis HP HPSBUX0312-304
Le CIAC a repris, sous la référence O-032, l'avis HP HPSBUX0312-304 au sujet de la création non sécurisée de fichiers temporaires par l'utilitaire 'shar'.
http://ciac.llnl.gov/ciac/bulletins/o-032.shtml
Reprise de l'avis Sun 57419
Le CIAC a repris, sous la référence O-033, l'avis Sun 57419 traitant d'une vulnérabilité lors de la création de fichiers temporaires permettant de créer ou d'effacer tout fichier présent sur le système.
http://www.ciac.org/ciac/bulletins/o-033.shtml
Reprise de l'avis Linux 'rsync'
Le CIAC a repris, sous la référence O-034, l'avis 'rsync' au sujet d'un débordement de buffer pouvant être exploité pour exécuter un code arbitraire.
http://www.ciac.org/ciac/bulletins/o-034.shtml
CAN-2003-0962
Reprise de l'avis Sun 57441
Le CIAC a repris, sous la référence O-035, l'avis Sun 57441 traitant d'une vulnérabilité dans 'dprintf' permettant d'exécuter un code arbitraire sous les droits 'root'.
http://www.ciac.org/ciac/bulletins/o-035.shtml
Reprise de l'avis Cisco 47184
Le CIAC a repris, sous la référence O-036, l'avis Cisco 47184 traitant d'un débordement de buffer dans ACNS pouvant autoriser un utilisateur distant à exécuter du code arbitraire.
http://www.ciac.org/ciac/bulletins/o-036.shtml
Reprise de l'avis Red Hat RHSA-2003:390
Le CIAC a repris, sous la référence O-037, l'avis Red Hat RHSA-2003:390 traitant d'une faille dans GnuPG autorisant un utilisateur à prendre connaissance de la clé privée ElGamal sign+encrypt de son correspondant.
http://www.ciac.org/ciac/bulletins/o-037.shtml
CAN-2003-0971
Reprise de l'avis Cisco 47186
Le CIAC a repris, sous la référence O-038, l'avis Cisco 47186 traitant des récentes installations de Cisco Unity sur serveurs IBM possédant des comptes utilisateurs et des adresses IP positionnés par défaut qu'il est nécessaire de supprimer ou de désactiver.
http://www.ciac.org/ciac/bulletins/o-038.shtml
Reprise de l'avis Cisco 47288
Le CIAC a repris, sous la référence O-039, l'avis Cisco 47288 traitant de deux vulnérabilités dans Cisco Firewall Services Module (FWSM) pouvant conduire à un déni de service.
http://www.ciac.org/ciac/bulletins/o-039.shtml
Reprise de l'avis Red Hat RHSA-2003:403
Le CIAC a repris, sous la référence O-042, les avis Red Hat RHSA-2003:403 et RHSA-2003:404 traitant des débordements de buffer dans le client ftp 'lftp' pouvant conduire à l'exécution de code arbitraire.
http://www.ciac.org/ciac/bulletins/o-042.shtml
CAN-2003-0963
FREEBSD
Disponibilité de plusieurs correctifs
FreeBSD annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquetages : bind FreeBSD-SA-03:19
http://www.linuxsecurity.com/advisories/freebsd.html
HP
Révision du bulletin HPSBUX0307-271
HP a révisé le bulletin HPSBUX0307-271 afin d'annoncer la disponibilité des correctifs pour HP-UX B.11.04, vulnérable à un déni de service dans certains programmes suite à un trafic réseau spécifique.
http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0307-271
Révision du bulletin HPSBUX0309-281
HP a révisé le bulletin HPSBUX0309-281 sur Sendmail afin d'annoncer la disponibilité des correctifs PHNE_29912 et PHNE_29913 pour HP-UX versions B.11.22 et B.11.23, correspondant à la version Sendmail 8.11.1. Ils corrigent un débordement de buffer exploitable à distance lors du traitement des en-têtes.
http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0309-281
CAN-2003-0694, CAN-2003-0681

Révision du bulletin HPSBUX0303-252

HP a révisé le bulletin HPSBUX0303-252 sur 'xdrmem_getbytes()' afin d'annoncer la disponibilité des correctifs PHCO_28480 et PHCO_28481 pour HP-UX versions B.11.00 et B.11.11. Ils corrigent un débordement de buffer dans la fonction 'xdrmem_getbytes()'.

<http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0303-252>

CAN-2003-0028

Révision du bulletin HPSBUX0310-291

HP a révisé le bulletin HPSBUX0310-291 sur OpenView Network Node Manager (NNM) afin d'annoncer la vulnérabilité des versions 5.02, 6.01, 6.10 et 6.31 pour environnement Microsoft Windows. Ce bulletin indique par ailleurs que les versions pour HP HP-UX et Sun Solaris ne sont pas vulnérables. HP annonce aussi la disponibilité de nouveaux correctifs.

<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0310-291>

Mise à jour du bulletin HP HPSBUX0311-303

HP a mis à jour son bulletin HPSBUX0311-303 concernant une vulnérabilité dans BIND pouvant conduire à un déni de service. Il annonce la disponibilité du correctif 'PHNE_30068' pour HP HP-UX B.11.11, remplaçant le correctif initial 'SSRT3653UX.depot'.

<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-303>

CAN-2003-0914

Correctifs pour 'OpenSSH'

HP a annoncé la disponibilité des correctifs pour OpenSSH pour HP-UX B.11.04 (VIVOS) avec Virtualvault A.04.60. Une vulnérabilité peut conduire à l'exécution de code arbitraire distant sous des droits privilégiés.

<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-302>

CAN-2003-0693

Correctifs pour BIND

HP a annoncé la disponibilité des correctifs pour BIND pour les versions HP-UX B.11.00 et B.11.11. Une vulnérabilité exploitable à distance permet de corrompre le cache DNS, provoquant ainsi un déni de service. <ftp://bind.bind1@hprc.external.hp.com/> Cependant, les fichiers annoncés dans le bulletin HP ('SSRT3653UX.depot' pour HP-UX B.11.11 et 'BIND812v005.depot' pour HP-UX B.11.00) ne coïncident pas avec ceux proposés dans le répertoire FTP. Notons par ailleurs que BIND 8.1.2 pour HP-UX B.11.00 atteindra sa fin de vie en mars 2004 et ne fera plus l'objet d'aucune mise à jour.

<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-303>

CAN-2003-0914

Révision du bulletin HPSBUX0309-281

HP a révisé le bulletin HPSBUX0309-281 afin d'annoncer de nouveaux correctifs pour HP-UX B.11.00, B.11.04, B.11.11, B.11.22 et B.11.23. Un débordement de buffer exploitable à distance lors du traitement des en-têtes par Sendmail permet d'obtenir les droits 'root'.

<http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0309-281>

CAN-2003-0694, CAN-2003-0681

Correctifs pour la bibliothèque CDE 'libdthelp.so'

HP a annoncé la disponibilité des correctifs pour la bibliothèque CDE 'libdthelp.so' pour HP Tru64 UNIX version 5.1. Un débordement de buffer permet d'acquérir des droits privilégiés.

<http://www.auscert.org.au/render.html?it=3660&cid=1>

CAN-2003-0834

Révision de l'alerte HPSBUX0311-295 sur JVM Classloader

HP a révisé l'alerte HPSBUX0311-295 sur Java VM Classloader pour préciser que la faille affecte HP-UX version 11.04 (VIVOS) avec Virtualvault A.04.50, A.04.60 ou A.04.70. Les correctifs sont disponibles.

<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-295>

Révision du bulletin HPSBUX0311-299 sur DCE

HP a révisé le bulletin HPSBUX0311-299 afin d'annoncer la disponibilité des correctifs pour HP-UX version B.11.23, vulnérable à un déni de service dans DCE.

<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-299>

HP/COMPAQ

Correctifs pour BIND sur Tru64

HP/COMPAQ a publié les correctifs pour HP Tru64 UNIX 4.0 et 5.1 éliminant la vulnérabilité dans BIND permettant de corrompre le cache DNS.

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0020650-V51BB24-ES-20031112>

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0020665-V51BB22-ES-20031113>

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0020675-V51AB24-ES-20031113>

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0020694-V51AB23-ES-20031114>

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0020695-V51B20-ES-20031114>

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT0020667-V40FB22-ES-20031113>

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT0020666-V40GB22-ES-20031113>

CAN-2003-0914

ISC

Dysfonctionnement dans BIND version 8.4.3

Une erreur dans BIND version 8.4.3 a conduit l'ISC à retirer cette version. Il ne s'agit pas d'un problème de sécurité mais peut, sous certaines conditions, générer un grand nombre de requêtes et avoir un impact opérationnel comparable à un déni de service. BIND 8.4.4 sera bientôt disponible. N'utilisez pas BIND 8.4.3 dans un environnement en production. La question de la présence de ce dysfonctionnement reste ouverte à l'ensemble des correctifs fournis par chaque éditeur annoncé vulnérable.

<http://www.isc.org/products/BIND/bind8.html>

IBM

Nouvelle clef GPG

IBM a publié un document informant de l'utilisation d'une nouvelle clef GPG pour signer tout mail émis par la liste AIX Security. Cette clef sera valide jusqu'au 15 décembre 2004. Les informations concernant l'obtention de la clef sont disponibles à l'adresse suivante :

<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1598.1>

<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1598.1>

Correctif pour BIND

IBM a publié le correctif APAR IY49881 pour AIX 5.1 éliminant la vulnérabilité dans BIND permettant de corrompre le cache DNS.

<http://www-1.ibm.com/support/docview.wss?uid=isq1IY49881>

CAN-2003-0914

LINUX DEBIAN

Disponibilité de nombreux correctifs

Debian annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquets :

kernel-image	DSA-403
rsync	DSA-404

<http://www.debian.org/security/2003/>

LINUX MANDRAKE

Disponibilité de nombreux correctifs

Mandrake annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquets :

gnupg	MDKSA-2003:109	9.0 / 9.1 / 9.2 / FW 8.2 / CS 2.1
kernel	MDKSA-2003:110	9.0 / 9.1 / FW 8.2 / CS 2.1
rsync	MDKSA-2003:111	9.0 / 9.1 / 9.2 / FW 8.2 / CS 2.1
cvs	MDKSA-2003:112	9.0 / 9.1 / 9.2 / FW 8.2 / CS 2.1
screen	MDKSA-2003:113	9.0 / 9.1 / 9.2 / FW 8.2 / CS 2.1
ethereal	MDKSA-2003:114	9.1 / 9.2
net-snmp	MDKSA-2003:115	9.1 / 9.2
lftp	MDKSA-2003:116	9.1 / 9.2 CS 2.1
irssi	MDKSA-2003:117	9.1 / 9.2
xfree-86	MDKSA-2003:118	9.1 / 9.2 CS 2.1

<http://www.linux-mandrake.com/en/security/>

LINUX REDHAT

Disponibilité de nombreux correctifs

RedHat annonce la disponibilité des correctifs corrigeant les vulnérabilités présentes dans les paquets :

kernel	RHSA-2003:392-01	7.1 / 7.2 / 7.3 / 8.0 / 9.0
net-snmp	RHSA-2003:335-01	8.0 / 9.0
rsync	RHSA-2003:398-01	7.1 / 7.2 / 7.3 / 8.0 / 9.0
gnupg	RHSA-2003:390-01	7.1 / 7.2 / 7.3 / 8.0 / 9.0
lftp	RHSA-2003:403-01	7.2 / 7.3 / 8.0 / 9.0
apache	RHSA-2003:320-01	8.0 / 9.0
apache	RHSA-2003:405-01	7.1 / 7.2 / 7.3

<http://www.linuxsecurity.com/advisories/redhat.html>

MICROSOFT

Complément d'informations sur l'usurpation de domaine

Un complément d'informations au sujet de la vulnérabilité affectant Microsoft Internet Explorer, Outlook et Outlook Express a été publié au travers de la base de connaissance de Microsoft et d'une alerte ISS X-Force. Cette dernière propose un outil s'intégrant au navigateur afin d'empêcher une exploitation de cette vulnérabilité.

<http://xforce.iss.net/xforce/alerts/id/159>

<http://support.microsoft.com/?id=833786>

MOZILLA

Usurpation de lien dans Mozilla

La vulnérabilité autorisant l'usurpation du domaine visité dans IE affecte aussi le navigateur Mozilla version 1.5. Les différences sont que le caractère '0x00' permet d'exploiter cette faille et que le lien usurpé apparaît lors du passage de la souris (événement 'MouseOver'). Ces vulnérabilités fonctionnent aussi bien via les protocole HTTP et HTTPS.

<http://www.securityfocus.com/bid/9203>

NOVELL

Correctif OpenSSL pour eDirectory

Novell a annoncé la disponibilité d'un correctif pour eDirectory version 8.7.1 et inférieures. Elle résoud les vulnérabilités découvertes dans OpenSSL.

<http://support.novell.com/cgi-bin/tidfinder/2967586>

CAN-2003-0543, CAN-2003-0544

NetBSD

Correctifs pour BIND

NetBSD a annoncé la disponibilité des correctifs pour BIND pour NetBSD version NetBSD 1.5 à 1.6.2_RC2 et current. BIND 8 est vulnérable à des attaques permettant de compromettre le cache DNS et conduisant à un déni de service.

<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-018.txt.asc>

<http://www.securityfocus.com/archive/1/347847>

CAN-2003-0914

ORACLE

Correctifs pour OpenSSL

Oracle a annoncé la disponibilité des correctifs pour OpenSSL éliminant de multiples vulnérabilités dans les implémentations SSL/TLS. Les versions suivantes sont affectées :

Oracle8i Database Server Release 3 V 8.1.7,

Oracle9i Database Server Release 1 V 9.0.1,

Oracle9i Database Server Release 2 V 9.2.0,

Oracle9i Application Server V 9.0.2 et 9.0.3,

Oracle9i Application Server Release 1 V 1.0.2.1s et 1.0.2.2, Oracle HTTP Server V 8.1.7, 9.0.1 et 9.2.

<http://otn.oracle.com/deploy/security/pdf/2003alert62.pdf>

CAN-2003-0544, CAN-2003-0545, CAN-2003-0543, CVE-2002-0082, CAN-2003-0078, CAN-2003-0147, CAN-2003-0131

SCO

Correctif pour BIND

SCO a publié un correctif pour SCO UnixWare 7.1.1 au sujet de la vulnérabilité dans BIND permettant de corrompre le cache DNS.

<ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.33/CSSA-2003-SCO.33.txt>

CAN-2003-0914

SGI

Correctif cumulatif pour SGI Advanced Linux

SGI a publié le correctif cumulatif 10039 pour sa plateforme SGI Advanced Linux ProPack v2.3, fixant ainsi les vulnérabilités dans 'pan', 'apache', 'wget' et 'gnupg'.

<ftp://patches.sgi.com/support/free/security/advisories/20031203-01-U.asc>

CAN-2003-0855, CAN-2003-0542, CAN-2002-1565, CAN-2003-0971

Correctifs noyau

SGI a publié des correctifs pour SGI ProPack v2.3 fixant une vulnérabilité dans la fonction 'do_brk()' permettant d'acquérir les droits 'root'.

<ftp://patches.sgi.com/support/free/security/advisories/20031201-01-A.asc>

CAN-2003-0961

Revision du bulletin SGI 20030904-01-P

SGI a révisé le bulletin 20030904-01-P au sujet de multiples vulnérabilités dans OpenSSL et OpenSSH. Il indique la disponibilité de nouveaux correctifs fixant un déni de service dans OpenSSL déclenché par la mauvaise gestion des séquences ASN.1, ainsi que des conflits de paquets suivant les versions de SGI IRIX.

<ftp://patches.sgi.com/support/free/security/advisories/20030904-02-P.asc>

Mise à jour du bulletin SGI 20031102-01-P

SGI a mis à jour son bulletin 20031102-01-P, concernant de multiples vulnérabilités dans le service 'rpc.mountd' du serveur NFS, pour indiquer la disponibilité des correctifs 5426, 5427, 5428 et 5429 remplaçant les correctifs 5387, 5388 et 5389.

<ftp://patches.sgi.com/support/free/security/advisories/20031102-02-P.asc>

CAN-1999-1225, CAN-2003-0796, CAN-2003-0797

Correctif pour 'rsync'

SGI a publié un correctif pour 'rsync' pour la plateforme SGI Advanced Linux ProPack v2.3, fixant ainsi un débordement de buffer permettant d'exécuter du code arbitraire.

<ftp://patches.sgi.com/support/free/security/advisories/20031202-01-U.asc>

CAN-2003-0962

Correctif cumulatif pour SGI Advanced Linux

SGI a publié un correctif cumulatif pour sa plateforme SGI Advanced Linux ProPack v2.3, fixant ainsi des vulnérabilités dans 'stunnel' et la bibliothèque 'glibc'.

<ftp://patches.sgi.com/support/free/security/advisories/20031103-01-U.asc>

CAN-2003-0740, CAN-2003-0689

SUN

Mise à jour du bulletin Sun 55221

Sun a mis à jour son bulletin 55221 concernant de multiples vulnérabilités affectant les serveurs d'application SunONE en environnement Windows. Il annonce la disponibilité de Sun ONE Application Server 7.0 Update Release 2 corrigeant les vulnérabilités dans les fonctions de journalisation et dans le moteur JSP.

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/55221>

Correctifs pour 'bash'

Sun a annoncé la disponibilité des correctifs pour Sun Cobalt Qube 3, RaQ 4 et RaQ XTR pour la vulnérabilité affectant l'interpréteur de commandes 'bash'. Celui-ci est vulnérable lors de l'utilisation de l'opérateur de redirection '<<'. Les fichiers temporaires créés ont un nom prévisible pouvant être utilisés dans des attaques par lien symbolique.

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/qube3.eng>

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq4.eng>

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raqxtr.eng>

CAN-2000-1134

Reprise de l'alerte BIND

Sun a publié sous la référence #57434 l'alerte concernant la compromission du cache dans BIND 8. Il annonce que le service 'in.named' fournit avec les plateformes Sun Solaris versions 7 à 9 (Sparc et x86) est vulnérable. Aucun correctif n'est pour l'instant disponible.

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57434>

CAN-2003-0914

Correctifs pour Apache et 'mod_ssl'

Sun a annoncé la disponibilité des correctifs pour Apache et 'mod_ssl' pour les versions Qube3, RaQ4, RaQ550 et RaQXTR.

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/qube3.eng>

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq4.eng>

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq550.eng>

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raqxtr.eng>

CAN-2003-0020, CAN-2003-0192

Correctifs pour Sendmail

Sun a annoncé la disponibilité des correctifs pour Sendmail sur RaQ4. Un débordement de buffer exploitable à distance lors du traitement des en-têtes par Sendmail permet d'obtenir les droits 'root'.

<http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/raq4.eng>

CAN-2003-0694, CAN-2003-0681

Correctif pour 'zebra'

Sun a annoncé la disponibilité d'un correctif pour 'zebra' pour Sun Linux 5.x corrigeant deux vulnérabilités pouvant conduire à un déni de service.

<http://sunsolve.sun.com/patches/linux/security.html>

CAN-2003-0795, CAN-2003-0858

Correctifs pour 'Ethereal'

Sun a annoncé la disponibilité des correctifs pour Ethereal pour Sun Linux 5.x. Ils fixent plusieurs débordement de buffer dans Ethereal exploitables via les dissecteurs 'GTP MSISDN', 'ISAKMP', 'MEGACO' et 'SOCKS'.

<http://sunsolve.sun.com/patches/linux/security.html>

CAN-2003-0925, CAN-2003-0926, CAN-2003-0927

TARANTELLA

Correctif pour OpenSSL

Tarantella a annoncé la disponibilité d'un nouveau Security Pack pour Tarantella Enterprise 3 versions 3.0 à 3.3. Il corrige une vulnérabilité dans OpenSSL lors traitement de la syntaxe ASN.1 pouvant conduire à un déni de service distant.

<http://www.tarantella.com/security/bulletin-08.html>

CAN-2003-0543, CAN-2003-0544, CAN-2003-0545

CODES D'EXPLOITATION

Les codes d'exploitation des vulnérabilités suivantes ont fait l'objet d'une large diffusion :

DAMEWARE

Code d'exploitation pour DameWare Mini Remote Control

Un code d'exploitation pour la vulnérabilité affectant DameWare Mini Remote Control versions inférieures à 3.73 a été publié. Il permet d'obtenir à distance un interpréteur de commandes sur Windows 2000 et XP sur lequel est installée une version vulnérable de DameWare. Les tentatives d'accès au port tcp/6129 utilisé par défaut par DameWare sont en augmentation.

<http://seclists.org/lists/fulldisclosure/2003/Dec/0617.html>

BULLETINS ET NOTES

Les bulletins d'information suivants ont été publiés par les organismes officiels de surveillance et les éditeurs :

ATTAQUES

Prévision des 'rituelles' attaques de fin d'année

Les fêtes de fin d'années sont une période propice aux attaques Internet. De récentes vulnérabilités n'étant toujours pas corrigées, le SANS encourage les utilisateurs à éteindre les machines non critiques afin de limiter les vecteurs de propagation des attaques. Par ailleurs, un grand nombre d'attaques par répliation ou 'phishing attacks' a été recensé. Leur but est de tromper l'utilisateur sur la légitimité du site visité, comme ici pour Visa.

<http://isc.sans.org/diary.html?date=2003-12-22>

<http://isc.sans.org/diary.html?date=2003-12-23>

Nouvelles techniques d'évasion de script

Plusieurs services de courrier électronique accessibles via le web sont vulnérables à de nouvelles techniques d'évasion de script. Il est donc possible de passer un script malicieux qui sera exécuté lors de la visualisation du mail. Excite, Outblaze et Yahoo! sont vulnérables lorsque le script est contenu entre deux balises spécialement construites : '<3CRIP>malicious code<3CRIP>' Il est possible de voir apparaître des virus exploitant cette faille.

http://www.finjan.com/news/press_show.cfm?press_release_id=124

<http://www.kb.cert.org/vuls/id/707100>

MICROSOFT

Publication de deux articles sur la faille Exchange

De nombreux cas concernant la vulnérabilité affectant Exchange Server 2003 et Outlook Web Access (OWA) ont été rapportés à Microsoft. L'installation de SharePoint Services 2.0 peut conduire à la désactivation de l'authentification Kerberos sur IIS. Il est alors possible d'accéder à la boîte aux lettres d'un utilisateur Exchange authentifié. Deux articles précisent la manière de corriger et d'éviter ce problème.

<http://support.microsoft.com/?id=832769> <http://support.microsoft.com/?id=832749>

<http://www.uniras.gov.uk/I1/I2/I3/brief2003/brief-64503.txt>

ATTAQUES

OUTILS

FTWALL - KAZAA

Description

Les infrastructures d'échange et de partage d'information peuvent être considérées comme une véritable nuisance lorsque celles-ci sont accédées par les salariés depuis leur poste de travail. Les protocoles utilisés – dits protocoles **P2P** ou **Peer-To-Peer** – sont considérés comme difficilement filtrables, et ce d'autant plus que chaque nouvelle version intègre généralement de nouvelles fonctionnalités visant à contourner les équipements de filtrage.

Direct Connect	412
Kazaa / Morpheus	1214
eDonkey / eMule	4662 à 4665, 4672-4673
GnuTella	6346 à 6347
Napster / WinMX	6699
BitTorrent	6881 à 6889

On restera cependant vigilant à régulièrement mettre à jour cette liste. Le port **1214** n'est ainsi plus obligatoirement utilisé par la toute dernière version de **'FastTrack'**, le protocole de communication de **'Kazaa'**. La version 2 peut en effet, et à l'instar des protocoles Gnutella et Napster, s'adapter dynamiquement au contexte.

Ainsi, en cas de filtrage du port **1214**, le client 'fournisseur' tentera de s'enregistrer sur le réseau **Kazaa** en utilisant un port destination normalement réservé à un protocole classiquement non filtré: le port 80 du service **HTTP**, le port 53 du service **DNS**, ... Ce canal sera ensuite maintenu ouvert afin d'obtenir le numéro de port ouvert par le client 'demandeur' dans l'hypothèse où la tentative de connexion de ce client serait rejetée par l'équipement de filtrage.

En pratique, la stratégie mise en œuvre est bien plus complexe et fait intervenir aussi bien les protocoles **UDP** que **TCP**. On retiendra que l'utilisation d'un canal de contrôle ouvert entre chaque client et le réseau **Kazaa** permet de déjouer la majorité des politiques de filtrage quitte à donner l'initiative de l'ouverture de la connexion de transfert au client 'fournisseur'.

C'est donc dans l'optique de garantir la fiabilité des mécanismes de filtrage que **Chris Lowth** a initié en juillet dernier le projet **'P2PWall'** dont l'objectif est le développement d'applications spécifiques de filtrage venant en complément du mécanisme **'IPTables'** bien connu des utilisateurs de l'environnement **LINUX**.

Dénommée **'FTWall'** (FastTrack Wall), la première application disponible permet de traiter le protocole **'FastTrack'**, et donc de gérer dynamiquement les applications utilisant celui-ci: **'Kazaa'** bien entendu mais aussi théoriquement tous les dérivés dont **KazaaLite**, **K++**, **iMesh**, **Grokster**, **WinMX**, **OpenNAP**, ...

La version 1 est annoncée avoir été testée avec succès face à **Kazaa** 2.1.1 et 2.5.1, **KazaaLite** 2.0.2, **K++** 2.4.3, **iMesh** 4.1 build 132 et 4.2 build 138, **Grokster** 1.7 et enfin **WinMX** 3.31.

La version 2 en cours de test intègre un mécanisme complémentaire permettant de bloquer le trafic en provenance des clients **WinMX** et **OpenNAP** en se référant au nom des serveurs contactés.

La complexité du protocole **'FastTrack'** a conduit l'auteur de **'FTWall'** à ne pas aborder le problème de front mais à biaiser en exploitant certaines spécificités de ce protocole.

L'idée générale est ainsi de leurrer le client afin de l'obliger à se maintenir dans le mode de fonctionnement le plus simple à traiter.

L'article publié sur le site **'LinuxJournal'** par **Chris Lowth** présente de manière détaillée le fonctionnement de **'FTWall'** face aux différentes situations qui peuvent être rencontrées.

Durant son initialisation, le client **'Kazaa'** transmet une série de paquets de reconnaissance **UDP** aisément identifiables. **'FTWall'** note les adresses IP source et destination puis transmet un paquet de réponse créé de toute pièce.

Ces fausses réponses conduisent le client à conclure à l'absence de filtrage et donc à continuer de tenter de contacter le réseau **'Kazaa'** dans ce mode.

Le tableau ci-contre récapitule ainsi les numéros de port TCP utilisés par les clients des principales applications d'échange et de partage de fichiers.

La mise en place de filtres destinés à rejeter les connexions effectuées à destination de ces ports depuis les clients internes reste recommandée à titre préventif.

Figures extraites de l'article publié dans **LinuxJournal**

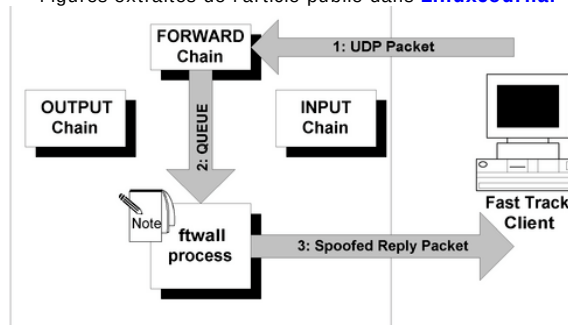


Figure 1. "opening shot" UDP packets

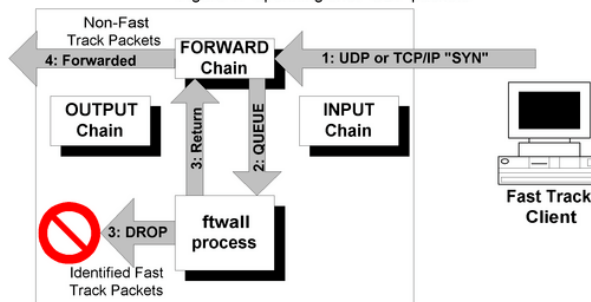


Figure 2. Other UDP and TCP/IP "SYN" Packets

En parallèle, le client va tenter d'ouvrir une connexion **TCP/IP** à destination de la cible dont l'adresse **IP** est désormais connue. **'FTWall'** peut alors rejeter les paquets **UDP** contenant cette adresse sans tenir compte du numéro de port et autoriser tous les autres paquets.

Le client va continuer de tenter de contacter d'autres points d'entrée dans le réseau **'Kazaa'** dont les adresses seront consignées par **'FTWall'**.

Au bout d'un certain temps, le client va changer de tactique et basculer dans un mode bien plus difficile à filtrer, le contenu des paquets étant chiffré et de multiples connexions **TCP** étant engagées en parallèle.

Dans ce mode et pour assurer le filtrage des adresses cibles non encore identifiées, **'FTWall'** va tout simplement interdire toute les tentatives d'ouverture d'un flux **TCP/IP** depuis le client, et ce pour une durée prédéfinie et réarmée par chaque tentative de connexion vers l'une des adresses cibles identifiées. Le revers de la médaille est que, bien entendu, le poste hébergeant le client **'Kazaa'** ne pourra plus du tout communiquer avec le monde extérieur du moins tant que le client reste actif.

En dernier recours, le client **'Kazaa'** va abandonner de nouveau ce mode pour tenter d'établir une session **TCP/IP** à la fois mais en augmentant considérablement le délai entre deux tentatives. Le mécanisme de protection précédent peut alors être mis en échec. La seule parade viable pour **'FTWall'** consiste à périodiquement tester la présence active du client **'Kazaa'** en lui transmettent un paquet **UDP** judicieusement construit. En cas de réponse, le filtrage **TCP** est maintenu.

L'article de **Chris Lowth** illustre parfaitement les tenants et aboutissants d'un marché non encore mature mais très prometteur s'il n'est pas rapidement contré sur le plan technique et/ou juridique. Tous les efforts des acteurs qui espèrent bien pouvoir contrôler durablement ce marché vont dans le même sens: contourner les obstacles et défaire les mécanismes de protection au risque de créer un système à terme incontrôlable et menaçant l'équilibre même de l'Internet.

• Complément d'information

<http://www.linuxjournal.com/article.php?sid=6945>
<http://p2pwall.sourceforge.net/>
http://www.ndnn.org/the_kazaa_problem.pptg
<http://www.kazaa.com/>
<http://www.kazaalite.nl>
<http://www.imesh.com>
<http://www.grokster.com/>
<http://www.winmx.com/>
<http://opennap.sourceforge.net/>

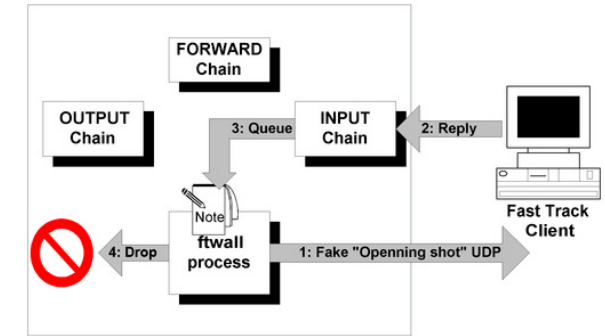


Figure 3. UDP Fast-track status probe

- Présentation de FTWall par son auteur
- Site FTWall
- Protocole d'échange FastTrack V2
- Infrastructure Kazaa
- Infrastructure KazaaLite / K++
- Infrastructure iMesh
- Infrastructure Grokster
- Infrastructure WinMX
- Infrastructure OpenNAP

DETESCAN / ANAPIRATE

• Description

Deux outils d'analyse de journaux développés par des universitaires Français ont attiré notre attention.

DeteScan

Présenté à l'occasion des **'Journées Réseaux 2003'**, l'utilitaire **'DeteScan'** vient au secours des exploitants en leur offrant la possibilité d'analyser rapidement les événements journalisés par les différents équipements réseaux afin de mettre en évidence les tentatives de sondages.

Résultant d'une collaboration entre plusieurs universitaires, cet utilitaire écrit en langage **'perl'** a pour principal avantage sa simplicité d'installation et d'utilisation. Sa mise en œuvre en environnement Linux ne nécessite en effet d'autre opération que la copie du fichier **'detescan.pl'** sur la machine centralisant les journaux et la configuration des quelques paramètres spécifiques au contexte: seuils d'alerte, adresse de messagerie collectant les résultats.

L'activation régulière de cet utilitaire par le biais d'un ordonnanceur permettra de disposer d'une vue synthétique des différentes sources de menace et d'engager les actions qui s'imposent. Le rapport d'analyse, transmis en format texte tabulé, liste les différentes sources de sondage puis détaille pour chacune d'elles, la liste des services objet de ce sondage.

Première section du rapport

Nov 30 05:44:22 : scan tcp de	host129-159.pool80116.interbusiness.it	sur le port 139 (netbios-ssn)	(16 machines)
Nov 30 06:02:39 : scan tcp de	host222-109.pool80181.interbusiness.it	sur le port 135 ()	(17 machines)
Nov 30 06:10:11 : scan tcp de	62-14-211-190.es.jazztelbone.net	sur le port 135 ()	(17 machines)
Nov 30 06:19:07 : scan icmp de	ac52.mistral.cz	de type icmp (8/0)	(17 machines)
...			
Nov 30 06:22:06 : scan tcp de	u209.d226215061.ctt.ne.jp	sur le port 135 ()	(15 machines)

Seconde section du rapport

Nov 30 06:19:07 : scan icmp de	ac52.mistral.cz	de type icmp (8/0)	(17 machines)
Nov 30 06:19:07 A.B.C.D 990423: 18w1d: %SEC-6-IPACCESSLOGDP: list 1 denied icmp A.B.C.E -> A.B.X.X (8/0), 1 packet			
...			
Nov 30 06:19:25 A.B.C.D 990432: 18w1d: %SEC-6-IPACCESSLOGDP: list 1 denied icmp A.B.C.E -> A.B.X.Z (8/0), 1 packet			

```
Nov 30 06:19:25 A.B.C.D 990433: 18w1d: %SEC-6-IPACCESSLOGDP: list 1 denied icmp A.B.C.E -> A.B.X.T (8/0), 1 packet
```

```
Nov 30 06:22:06 : scan tcp de u209.d226215061.ctt.ne.jp sur le port 135 ( ) ( 15 machines )
```

Le lecteur en conviendra, le format de présentation est ici réduit au strict minimum mais il permet de mettre rapidement en évidence l'importance et la durée d'une vague de sondage. Comme précédemment mentionné, la mise en œuvre de **'detescan.pl'** est immédiate et sans difficulté aucune, du moins lorsque le format des enregistrements traités est celui spécifié par défaut pour l'équipement.

Nous avons ainsi dû légèrement modifier le code pour traiter les enregistrements générés par un routeur Cisco insérant l'identification de l'interface dans les enregistrements, cas de figure a priori non prévu par les auteurs de l'utilitaire !

```
Nov 30 05:36:33 X.Y.Z.T 990246: 18w1d: %SEC-6-IPACCESSLOGP:
```

```
list ExterneInterne denied tcp A.B.C.D(4318) (FastEthernet0/0 0008.21be.d560) -> X.Y.Z.T(445), 1 packet
```

L'utilitaire **'DeteScan'** supporte une impressionnante liste d'équipements: routeurs **Cisco**, **Allied Telesys**, **Foundry**, **Cabletron**, **Extreme Networks**, pare-feu et Filtres **Cisco PIX**, **screend**, **ipchain**, **iptables** et enfin la sonde de détection d'intrusion **snort**. Sa conception conduit cependant à réserver son utilisation pour l'analyse de journaux d'un volume raisonnable, les auteurs annonçant en effet une occupation mémoire de 676Mo durant l'analyse de 2 millions d'enregistrements contenant 900 000 rejets.

AnaPirate

Développé par Luc Veillon de l'**IRD** – Institut de Recherche et de Développement – l'outil **'AnaPirate'** permet d'automatiser la tâche fastidieuse de recherche des tentatives d'accès illicites et de notification des entités compétentes: le service **'abuse'** du fournisseur d'accès et si besoin le **CERT** le plus proche.

Constitué d'une dizaine de fichiers dont 6 bibliothèques **'perl'**, le paquetage **'AnaPirate'** nécessite une phase de configuration avant utilisation requérant l'édition:

- du fichier principal pour le positionnement éventuel des seuils d'alerte par défaut, ces seuils pouvant être modifiés directement sur la ligne de commande,
- du fichier de configuration pour la sélection des sources de données qui seront prises en compte dans l'analyse. Sont actuellement reconnus les journaux générés par les routeurs **CISCO**, par le serveur **Apache** et enfin par le système d'exploitation **Solaris**. On notera toutefois quelques restrictions fonctionnelles en ce qui concerne le traitement des deux dernières sources. Ce fichier de configuration contient par ailleurs la liste des serveurs **'whois'** qui seront interrogés pour déterminer les points de contact des entités à notifier.
- de l'ensemble des modèles des lettres qui seront automatiquement transmises aux entités. Le premier modèle correspond au message transmis au service responsable du traitement des plaintes pour l'adresse concernée, le second au modèle de message transmis au(x) CERT(s).

Cet outil, destiné à être régulièrement activé sur les journaux, génère une impressionnante quantité de courriers. Ainsi, le traitement de la journalisation des événements collectés en 24 heures sur le point d'accès réservé à notre service de veille conduit à la génération de plus de 410 courriers.

Cet important volume est principalement dû au mode de fonctionnement retenu consistant à envoyer un courrier pour chaque source de nuisance sans agréger ceux-ci par service destinataire. Le volume généré peut être partiellement réduit en modifiant les deux paramètres descriptifs des seuils de notification applicables à chaque source :

- **level_warning** (option **-s**) spécifiant le nombre minimum de sondages requis pour envoyer une notification,
- **packet_warning** (option **-p**) indiquant le nombre minimum de paquets devant être reçus pour une notification.

Nos tests mettent en évidence la difficulté que l'on rencontrera pour trouver le compromis idéal, c'est à dire le paramétrage minimisant le volume de courrier à retransmettre tout en conservant les sources de nuisance les plus sévères. Dans nos exemples, le positionnement de seuils à 20 et 80 (resp. **level_warning** et **packet_warning**) a permis de réduire le volume de message de **410** à **73**, ces paramètres étant configurés par défaut à 5 et 10 dans le code (et non à 10 et 50 comme le laisse entendre la documentation).

Il est en conséquence fortement recommandé de démarrer sur un petit fichier de journalisation en mode 'manuel' (mode pour lequel les courriers sont transmis sur une adresse de test) afin d'optimiser la configuration des seuils. L'option autorisant la transmission automatique de ces courriers aux services concernés pourra ensuite être activée.

Exemple d'un courrier transmis au service 'abuse'

```
Our REF : 2003/67
Dest : abuse@t-ipnet.de, postmaster@dip.t-dialin.net
For Deutsche Abuse, Generic email
Dear colleague(s),
We have seen a host from your domain, 217.224.249.62 (pd9e0f93e.dip.t-dialin.net)
scanning port(s) tcp(135)
beginning at : 01/12/2003 07:01:07 GMT+01:00 NTP synchronized,
ending at : 01/12/2003 07:01:14
on these addresses in our networks :
62.A.B.14,16-31
```

or, if you prefer more details :

DD/MM/YYYY HH:MM:SS to DD/MM/YYYY HH:MM:SS	IP src	IP dst	Service dst
01/12/2003 07:01:07 to 01/12/2003 07:01:07	217.224.249.62	62.A.B.14	tcp(135)
01/12/2003 07:01:08 to 01/12/2003 07:01:08	217.224.249.62	62.A.B.16	tcp(135)
01/12/2003 07:01:08 to 01/12/2003 07:01:08	217.224.249.62	62.A.B.17	tcp(135)
01/12/2003 07:01:08 to 01/12/2003 07:01:08	217.224.249.62	62.A.B.18	tcp(135)
01/12/2003 07:01:07 to 01/12/2003 07:01:07	217.224.249.62	62.A.B.19	tcp(135)
01/12/2003 07:01:08 to 01/12/2003 07:01:08	217.224.249.62	62.A.B.20	tcp(135)
01/12/2003 07:01:14 to 01/12/2003 07:01:14	217.224.249.62	62.A.B.21	tcp(135)
01/12/2003 07:01:13 to 01/12/2003 07:01:13	217.224.249.62	62.A.B.22	tcp(135)
01/12/2003 07:01:13 to 01/12/2003 07:01:13	217.224.249.62	62.A.B.23	tcp(135)
01/12/2003 07:01:13 to 01/12/2003 07:01:13	217.224.249.62	62.A.B.24	tcp(135)
01/12/2003 07:01:13 to 01/12/2003 07:01:13	217.224.249.62	62.A.B.25	tcp(135)
01/12/2003 07:01:13 to 01/12/2003 07:01:13	217.224.249.62	62.A.B.26	tcp(135)
01/12/2003 07:01:13 to 01/12/2003 07:01:13	217.224.249.62	62.A.B.27	tcp(135)
01/12/2003 07:01:14 to 01/12/2003 07:01:14	217.224.249.62	62.A.B.28	tcp(135)
01/12/2003 07:01:14 to 01/12/2003 07:01:14	217.224.249.62	62.A.B.29	tcp(135)
01/12/2003 07:01:14 to 01/12/2003 07:01:14	217.224.249.62	62.A.B.30	tcp(135)
01/12/2003 07:01:13 to 01/12/2003 07:01:13	217.224.249.62	62.A.B.31	tcp(135)

We would appreciate any help to find the author of this scanning, and to stop his activity against our institute. Could you help us by searching some information about that host in your log files ?

Thank-you for your help

Best regards

My Name and Surname | My company
 tel.:+33(0)X XX XX XX XX | Responsable securite / Security Manager
 Fax :+33(0)Y YY YY YY YY | 1, my street
 my@email | MY TOWN

This mail was powered by anapirate :

<http://www.orleans.ird.fr/pub/anapirate/anapirate-site.html>

Exemple d'un courrier transmis au(x) CERT(s)

Subject: [ANAPIRATE CERT summary]

#Rapport anapirate concernant les sites de la société Apogee communications

#Seuils d'alarme : 10 lignes log cisco ou 50 packets

#Masques lignes ignorees sample/ignore.cert

#DD/MM/YYYY HH:MM:SS to DD/MM/YYYY HH:MM:SS	IP src	IP dst	Service dst	Nbre
30/11/2003 18:09:31 to 30/11/2003 18:09:31	12.135.198.196	62.A.B.24	tcp(445)	1
30/11/2003 09:05:55 to 30/11/2003 09:09:31	12.154.97.136	62.A.B.23	tcp(135)	12
30/11/2003 09:06:16 to 30/11/2003 09:09:31	12.154.97.136	62.A.B.23	tcp(445)	14
30/11/2003 22:36:40 to 30/11/2003 22:38:42	12.154.97.136	62.A.B.27	tcp(135)	11
30/11/2003 22:37:01 to 30/11/2003 22:38:42	12.154.97.136	62.A.B.27	tcp(445)	11
01/12/2003 23:40:27 to 01/12/2003 23:40:27	12.159.175.242	62.A.B.26	udp(1026)	1
01/12/2003 03:17:46 to 01/12/2003 03:17:46	12.215.155.52	62.A.B.21	tcp(445)	1
30/11/2003 09:23:07 to 30/11/2003 09:23:07	12.215.212.78	62.A.B.14	tcp(135)	1
30/11/2003 09:23:08 to 30/11/2003 09:23:08	12.215.212.78	62.A.B.29	tcp(135)	1
...				
02/12/2003 03:30:01 to 02/12/2003 03:30:01	82.82.153.4	62.23.184.24	tcp(21)	1
02/12/2003 03:30:16 to 02/12/2003 03:30:16	82.82.153.4	62.23.184.25	tcp(21)	2

My Name and Surname | My company
 # tel.:+33(0)X XX XX XX XX | Responsable securite / Security Manager
 # Fax :+33(0)Y YY YY YY YY | 1, my street
 # my@email | MY TOWN

This mail was powered by anapirate :

<http://www.orleans.ird.fr/pub/anapirate/anapirate-site.html>

Extrait du rapport de synthèse

#Seuils d'alarme : 5 lignes log cisco ou 10 packets

#Masques lignes ignorees sample/ignore.cert

#DD/MM/YYYY HH:MM:SS to DD/MM/YYYY HH:MM:SS	IP src	IP dst	Service dst	Nbre
30/11/2003 18:09:31 to 30/11/2003 18:09:31	12.135.198.196	62.A.B.24	tcp(445)	1
30/11/2003 09:05:55 to 30/11/2003 09:09:31	12.154.97.136	62.A.B.23	tcp(135)	12
30/11/2003 09:06:16 to 30/11/2003 09:09:31	12.154.97.136	62.A.B.23	tcp(445)	14
30/11/2003 22:36:40 to 30/11/2003 22:38:42	12.154.97.136	62.A.B.27	tcp(135)	11
30/11/2003 22:37:01 to 30/11/2003 22:38:42	12.154.97.136	62.A.B.27	tcp(445)	11
01/12/2003 03:17:46 to 01/12/2003 03:17:46	12.215.155.52	62.A.B.21	tcp(445)	1
30/11/2003 09:23:07 to 30/11/2003 09:23:07	12.215.212.78	62.A.B.14	tcp(135)	1
...				
02/12/2003 10:37:05 to 02/12/2003 10:37:05	82.64.76.2	62.A.B.30	tcp(135)	1
02/12/2003 10:38:05 to 02/12/2003 10:38:05	82.64.76.2	62.A.B.31	tcp(135)	1
02/12/2003 03:30:01 to 02/12/2003 03:30:01	82.82.153.4	62.A.B.24	tcp(21)	1
02/12/2003 03:30:16 to 02/12/2003 03:30:16	82.82.153.4	62.A.B.25	tcp(21)	2

A l'usage, 'AnaPirate' s'avère offrir une très intéressante visibilité sur les tentatives d'accès illicites dont la volumétrie est généralement masquée par les regroupements opérés par les outils traditionnels que ce soit 'detescan' ou encore le remarquable outil 'fwlogwatch' (Rapport N°53 – Décembre 2002).

On notera l'absence de quelques fonctionnalités qui seraient pourtant bien utiles dans le contexte d'utilisation de ce type d'outil et notamment la possibilité de :

- Visualiser l'avancement du traitement lorsque celui-ci est activé depuis une console et non en arrière plan,
- Masquer les adresses locales dans le rapport destiné à être transmis aux CERTs quand bien même celles-ci sont publiques,
- Signer les messages transmis à l'attention des services tiers, voire chiffrer le rapport transmis aux CERTs. Le format actuellement utilisé est le format de remontée d'incident spécifié par le CERT **Renater**.

L'utilitaire 'AnaPirate' devient rapidement indispensable à qui souhaite prendre une part active dans l'éradication des systèmes infectés à l'origine de la majorité des nuisances actuellement rencontrées. L'incroyable gain de temps offert par cet outil ne devra cependant pas faire oublier qu'il peut lui aussi devenir rapidement une nuisance pour les autres lorsqu'il est employé en mode 'automatique' s'il n'est pas correctement configuré et son fonctionnement régulièrement contrôlé. En effet, la stratégie de détermination des services à contacter ne peut être considérée comme parfaitement fiable. Elle peut conduire à envoyer un ou plusieurs messages de notification sur la boîte à lettre d'un tiers non directement concerné qui verra d'un mauvais œil une sollicitation qui pourrait s'apparenter à du SPAM.

La stratégie actuellement mise en œuvre consiste à interroger les bases 'Whois' sur l'adresse IP ou le nom de domaine à l'origine de la nuisance et à récupérer les adresses de messagerie contenues dans les champs 'TechEmail:', 'OrgTechEmail:', 'OrgAbuseEmail:', 'e-mail:' de l'enregistrement 'person' ou indiquées dans le champ 'E-mail:' de l'enregistrement 'Abuse'. Le format spécifique au serveur 'whois.cyberabuse.org' est parfaitement géré. Les systèmes pour lesquels aucun point de contact n'a pu être découvert sont listés dans le rapport généré après chaque activation de l'utilitaire. Aucun message de notification n'est créé pour les incidents ayant pour origine ces systèmes.

Cette stratégie ne prend hélas pas en compte les informations contenues dans certains champs d'information. Ainsi, l'analyse de la réponse 'whois', dont un extrait est présenté ci-dessous, conduira à envoyer une notification à l'adresse 'hostmaster@mistral.cz' quand l'adresse devant être utilisée est 'abuse@mistral.cz' ...

inetnum:	62.24.72.0 - 62.24.87.255
netname:	DATTELKABEL-II
descr:	UPC Internet CATV
remarks:	*****
remarks:	* In case of hack attacks, scans etc. please *
remarks:	* send abuse notifications to: *
remarks:	* abuse@mistral.cz *
remarks:	*****
remarks:	* In case of spam please send abuse *
remarks:	* notifications to: *
remarks:	* spam@mistral.cz *
remarks:	*****
route:	62.24.80.0/22
descr:	UPC Ceska republika, a.s.
mnt-by:	DKI-MNT
changed:	martin.kxxxxxxx@upc.cz 20021111
source:	RIPE
role:	Mistral Contact Role
address:	UPC Ceska republika, a.s.
phone:	+ 420 2 61107111
fax-no:	+ 420 2 61107100
e-mail:	hostmaster@mistral.cz
trouble:	+-----+ customer contact Mistral Hotline 420 2 41005372 customer contact Mistral Hotline Brno 420 844 111372 +-----+
changed:	hostmaster@mistral.cz 20030612
source:	RIPE
person:	Martin Kxxxxxxx
address:	UPC Ceska republika, a.s.
fax-no:	+420 2 61107100
e-mail:	hostmaster@mistral.cz
nic-hdl:	MK23104-RIPE
notify:	hostmaster@mistral.cz
mnt-by:	DKI-MNT
changed:	hostmaster@mistral.cz 20030710
source:	RIPE

On comprendra l'importance du bon usage des enregistrements **Whois** et de la mise à jour régulière de ceux concernant les adresses des contacts techniques et administratifs, adresses qui ne sont plus obligatoirement nominatives mais peuvent être attachées à un rôle.

Nous concluons cette rapide présentation par tableau récapitulatif des équipements supportés par ces deux produits et 'fwlogwatch'.

	fwlogwatch	detescan	anapirate
Routeur	CISCO IOS LanCom	CISCO IOS Allied Telesys, Foundry, Cabletron, Extreme Networks	CISCO IOS
UNIX	ipfilter	TrueUnix screend	Syslog Solaris 2.6 et 2.7
Firewall	CISCO PIX Netscreen	CISCO PIX	
IDS	snort	snort	
Linux	ipchain iptables	ipchain iptables	
Windows	Windows XP ICF		
Autre			apache

■ Complément d'information

<https://www.orleans.ird.fr/pub/anapirate/anapirate-site.html>

<http://www.igh.cnrs.fr/perso/denis.pugnere/detescan>

<http://cert.uni-stuttgart.de/projects/fwlogwatch/>

<http://www.sawmill.net/index.html>

- AnaPirate

- Detescan

- FwLogWatch

- SawMill

TECHNIQUES

MALWARE

■ Description



Le site personnel de **Jarkko Turkulainen** nous propose une analyse détaillée de deux portes dérobées assez récentes: '**BackDoor.Dewin.k**' et '**BackDoor.Spotcom**'. Pour mémoire, le rôle d'un tel logiciel est d'autoriser le contrôle à distance du système sur lequel il a été – généralement illicitement – installé.

Pour être exploitable le plus longtemps possible, et comme son nom l'indique, une porte dérobée devra être conçue pour masquer son activité sur le système compromis mais aussi dans l'environnement d'accueil de celui-ci. Les codes actuels – qu'il s'agisse de portes dérobées, de vers ou de virus - intègrent ainsi plusieurs mécanismes permettant de les rendre invisibles:

- Manipulation des structures du système pour masquer l'activité générée par l'exécution et dissimuler les modifications effectuées sur le système lors de l'installation,
- Dissimulation des communications en réutilisant un protocole connu afin de noyer les données échangées dans la masse et de passer à travers les dispositifs de filtrage,
- Modification du comportement par téléchargement régulier de mises à jour partielles ou totales du code.

Les deux portes dérobées étudiées par **Jarkko Turkulainen** sont conformes à ce modèle. Elles sont particulièrement intéressantes du point de vue du protocole de communication et de la technique de dissimulation. Nous invitons le lecteur à lire les deux analyses disponibles sur le site de l'auteur en proposant cependant un tableau de synthèse des caractéristiques des deux codes.

	BackDoor.Dewin.k	BackDoor.Spotcom
Taille du code	46 Ko	37 Ko
Compressé	Format 'PE Compact'	Format 'UPX'
Langage	C/C++	Non spécifié
Image	Nom d'un service existant (svchost.exe)	Remplace le service ' QoS RSVP ' (rsvp.exe)
Dissimulation	Masquage derrière le nom d'un service connu	Insertion dans une instance masquée de IE
Modèle	Reverse: Connexion sortante vers serveur	Reverse: Connexion sortante vers serveur
Protocole	Protocole HTTP	Protocole spécifique sur le service DNS
Serveur	Paramétrable par script	Fixé à 218.242.252.211
Modularité	Actions via langage de scripting	Téléchargement de fichiers
Commandes	19 commandes natives dont : - GetURL() - Sleep() - Update() - AddServer() - Get_Reg() - Set_Reg()	6 commandes natives : - Synchronize() - TimeOut() - Listen() - Connect() - Monitor() - GetFile()

La technique de dissimulation employée par ces deux codes repose sur la confusion susceptible d'être créée dans l'esprit de l'utilisateur par l'emploi d'un nom d'application déjà connu et directement associé à des communications réseaux.

Ainsi, le choix du nom '**svchost.exe**' par la porte dérobée '**Dewin**' offre une couverture idéale. Ce nom désigne en effet une application générique dénommée '**Generic Host Process for Win32 Services**' destinée à servir de support aux services Internet implémentés sous la forme d'une librairie dynamique (partages réseaux, accès distants, ...). Aucune information concernant le service associé à chaque instance de cette application n'étant délivrée par les outils d'administration, on comprendra la difficulté que rencontrera un utilisateur à séparer le grain de l'ivraie.

Le concepteur de la seconde porte dérobée a choisi une voie alternative plus compliquée sur le plan de la programmation. Une instance masquée du navigateur **Internet Explorer** est exécutée puis le code de la porte dérobée contenu dans une librairie dynamique est greffé sur cette instance en utilisant les fonctions ad'hoc offertes par le système Windows. L'utilisateur remarquera tout au plus l'existence d'un processus correspondant à une instance du navigateur et n'en sera pas alarmé à moins de ne jamais avoir ouvert ce navigateur.

Nombre de situations de ce type pourraient être évitées par la mise à disposition d'outils ergonomiques et fiables permettant de visualiser les ressources associées à un processus, dans le cas présent l'**URL** traitée par le navigateur '**Internet Explorer**' et le nom de la librairie de service hébergée par le service '**svchost**'. Fort heureusement, Microsoft semble avoir pris en compte ce besoin dont tout laisse à penser qu'il pourrait bien être intégré dans les tous prochains services pack.

• Complément d'information

<http://www.klake.org/~jt/malware/>

<http://www.sysinternals.com/ntw2k/freeware/procexp.shtml>

- Articles de 'Jarkko Turkulainen'

- Process Explorer

DIGRESSIONS AUTOUR DE L'ENCODAGE ASN.1

• Description



Le **NISCC** – centre anglais de coordination des problèmes de sécurité – a publié mi-novembre un très intéressant article accompagnant la diffusion de trois alertes ayant pour point commun le traitement incorrect des structures de données encodées au format **ASN.1** par de nombreuses implémentations protocolaires dont **X400**, **SMIME** et **SSL**.

En 2001, le groupe de recherche en sécurité informatique de l'université finlandaise de **Oulu** démarrait le projet '**PROTOS**' destiné à valider le comportement d'un protocole de communication à qui l'on soumettrait des structures de données incohérentes.

Les résultats désastreux de la première campagne de test effectuée sur le protocole **LDAP** publiés en juillet 2001 passaient quasiment inaperçus en dehors de la diffusion de l'avis **CA-2001-18** du **CERT-CC**. La faible diffusion de ce protocole, à l'époque, peut expliquer cela.

En février 2002, l'équipe du projet publiait les résultats des tests menés sur de nombreuses implémentations du célèbre protocole d'administration réseau **SNMP**, déjà connu pour ne pas être un modèle du genre en matière de sécurité. Démontrant par la pratique qu'aucune des implémentations testées n'était capable de gérer correctement et sans risque les situations d'exception auxquelles elles étaient soumises, ces résultats ont immédiatement fait la Une de la presse spécialisée et des organismes d'alerte : avis du **CERT-CC CA-2002-03**, du **SANS**, ...

Il aura ainsi fallu 6 mois et le choix d'engager une campagne de validation portant sur un protocole connu et largement diffusé pour que soit enfin étalé au grand jour un problème pourtant connu de longue date des spécialistes de la validation et des personnels des services qualité.

Doit-on rappeler qu'à l'époque désormais révolue des protocoles **OSI**, les éditeurs étaient tenus de faire valider leur implémentation auprès d'un centre de test – **CTS** ou **Conformance Testing Service** - pour se voir délivrer un certificat de conformité. De notre point de vue, la situation dénoncée en 2002 par les universitaires d'Oulu et aujourd'hui par le **NISCC** résulte tout simplement de la stratégie engagée par le **DARPA** dans les années 80 autour des technologies qui devaient donner le jour à l'Internet. Pilotée par des universitaires, et répondant à des contraintes purement tactiques dont notamment celle de disposer d'une infrastructure de communication résiliente, cette stratégie a conduit insidieusement à l'établissement de standards de fait, généralement incomplets et souvent inadaptés aux besoins réels des professionnels.

On ne peut hélas refaire le monde, et c'est dans cette logique que s'inscrit l'article du **NISCC** intitulé fort à propos '**Working together to beat vulnerabilities**'. Travaillons en effet ensemble pour combattre les vulnérabilités, ou plus précisément, définissons en commun les cibles devant prioritairement faire l'objet d'une campagne de validation similaire à celles engagées par l'équipe de l'université d'Oulu. C'est en ces termes que le **NISCC** présente le projet ayant permis de sélectionner les protocoles **X400**, **SMIME**, **SSL** et mené à l'identification des vulnérabilités précitées.

Les résultats obtenus par le **NISCC** sont forts intéressants. Ils ont non seulement permis d'identifier un mode de défaillance commun à ces trois protocoles – l'encodage de la syntaxe **ASN.1** - mais aussi de mettre en défaut l'idée reçue que l'utilisation d'un langage de description des données puisse renforcer la résilience d'une application vis à vis de données mal formatées.

Un rapide historique de la genèse de la syntaxe **ASN.1** permettra de mieux comprendre les problèmes découverts par le **NISCC**, le lecteur étant par ailleurs invité à lire la remarquable présentation intitulée '**A layman's guide to a subset of ASN.1, BER and DER**' publiée il y a quelques années – 1993 - par la société '**RSA Inc.**'

Contrairement aux protocoles développés autour des réseaux **DARPA** dont la syntaxe était intelligible par un être humain, les concepteurs des protocoles **OSI** ont opté pour l'utilisation de structures de données normées et définies par le biais d'un langage de description dit **ASN.1** ou 'Abstract Language Notation Number 1' (norme ISO 8824).

Ce langage autorise la définition de types de données évolués à partir d'un ensemble de types élémentaires tels que 'INTEGER' pour un entier, 'SEQUENCE OF' pour une collection ordonnée d'objets ou encore 'OBJECT IDENTIFIER' pour un identifiant d'objet.

L'extrait de la définition des objets spécifiés par la norme X9-84-CMS présenté ci-dessous permet de visualiser leur construction.

```
SignedData ::= SEQUENCE {
    version          CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates[0]   CertificateSet OPTIONAL,
    crls[1]           CertificateRevocationLists
OPTIONAL,
    signerInfos      SignerInfos
}
SignerInfo ::= SEQUENCE {
    version          CMSVersion,
    sid              SignerIdentifier,
    digestAlgorithm   DigestAlgorithmIdentifier,
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signature         SignatureValue
}
SignatureAlgorithmIdentifier ::=
    AlgorithmIdentifier { { SignatureAlgorithms } }
SignatureAlgorithms ALGORITHM ::= {
    { OID dsa-with-sha1          PARMS NoIV } |
    { OID ecdsa-with-SHA1       PARMS NoIV } |
    { OID sha1WithRSASignature PARMS NoIV },
    ...
}
```

La caractéristique unique de cette approche est d'avoir spécifié une structure permettant d'organiser et de référencer chacun des objets ainsi créés par le biais d'un identifiant construit en tenant compte de la hiérarchie de l'objet dans l'organisation de la structure.

Il devient alors possible de référencer une structure par la seule connaissance de cet identifiant dit 'OID' ou 'Object Identifier'.

La définition **ASN.1** d'un objet – une clef publique par exemple - indique sa structure mais ne précise rien sur le plan du codage des données lors du transfert de l'objet entre deux entités.

Cet encodage est spécifié dans les normes **ISO.8824/X.208 'Specification of Abstract Syntax Notation One'** et **ISO.8825/X.209 'Specification of Basic Encoding Rules for Abstract Syntax Notation One'**. S'appuyant sur un formalisme de type 'TLV' ou 'Type – Longueur – Valeur', ces normes distinguent deux méthodes d'encodage :

- La première méthode, dite 'BER' ou 'Basic Encoding Rules' autorise l'encodage d'une même donnée de plusieurs manières en jouant notamment sur l'encodage du champ réservé à la longueur. L'exemple ci-après – repris du guide précité - met en évidence les différentes possibilités d'encodage d'une simple valeur numérique.

La chaîne de caractères 'APOGEE' peut ainsi être encodée sous la forme d'une chaîne simple :

Type	Longueur	A	P	O	G	E	E
0x16	0x06	0x41	0x50	0x4F	0x47	0x45	0x45
0x16	0x81	0x06	0x41	0x50	0x4F	0x47	0x45

Forme concise
Forme étendue

mais aussi de la succession de sous-chaînes de forme concise :

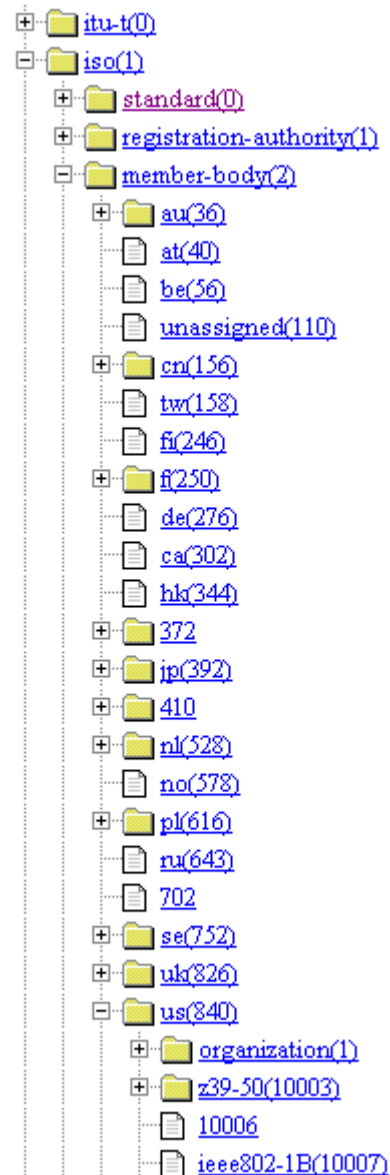
Type	Longueur	A	P	O	G	E	E
0x36	0x0C						
0x16	0x02	0x41	0x50				
0x16	0x02			0x4F	0x47		
0x16	0x02					0x45	0x45

Séquence de
Forme concise
Forme concise
Forme concise

Ou d'une combinaison de formes :

Type	Longueur	A	P	O	G	E	E
0x36	0x81 0x0E						
0x16	0x81 0x02	0x41	0x50				
0x16	0x81 0x02			0x4F	0x47		
0x16	0x02					0x45	0x45

Séquence de
Forme étendue
Forme étendue
Forme concise



On imagine sans peine la complexité de la fonction d'encodage qui doit impérativement connaître la taille de chacun des éléments préalablement à l'encodage, et celle de la fonction de décodage qui doit pouvoir traiter tous les cas possibles en rejetant les encodages non conformes. Cette méthode est cependant celle utilisée par la quasi-totalité des protocoles requérant l'usage de structures **ASN.1**.

- La seconde méthode, dite '**DER**' ou '**Distinguished Encoding Rules**', simplifie quelque peu le travail des fonctions d'encodage et de décodage en imposant l'utilisation d'une forme d'encodage, la forme concise ou '**Short Form**' dans le cas d'une donnée dont la taille est compatible avec le stockage de la longueur sur un octet, la forme étendue ou '**Long Form**' dans les autres cas.

Bien qu'aucune information précise ne soit fournie dans les alertes émises par l'**UNIRAS**, il est fort probable que les problèmes mis en évidence par le **NISCC** proviennent des fonctions de décodage des structures encodées '**BER**', traitements ne prenant généralement pas en compte les 'irrégularités' d'encodage.

Force est de constater que nombre de bibliothèques de décodage librement accessibles ont été développées en considérant que les paramètres fournis sont correctement structurés, les erreurs d'intégrité ayant normalement été corrigées par la couche de service sous-jacente. Rappelons en effet que ces bibliothèques ont été développées dans le cadre des protocoles **OSI**.

Cette brève présentation du langage de description **ASN.1** et de ses particularités nous permet d'aborder un sujet plus rarement traité, pour ne pas dire confidentiel. La complexité inhérente à l'encodage '**ASN.1**' impacte directement les dispositifs de filtrage ou de sécurité devant inspecter le contenu du flux de données pour déterminer les règles applicables.

S'il est aisé de traiter les flux de données pour lesquels les éléments pertinents se trouvent à des positions fixes et immuables, il en va tout autrement avec les flux comportant des données encodées en '**BER**' ou '**DER**', et plus largement sous une forme 'Longueur/Valeur'. Le système de filtrage doit alors intégrer les fonctions de décodage pour assurer pleinement sa fonction, et ce au détriment des performances et avec les risques que l'on sait désormais si les données ne sont pas encodées correctement.

Le concepteur de tels systèmes est alors confronté au dilemme suivant :

- décoder totalement le flux de données avec une perte de performance conséquente et une possibilité non négligeable d'atteinte en déni de service,
- décoder le flux de données de manière 'approximative' en acceptant le risque d'autoriser certains flux normalement interdits.

Cette dernière option est généralement retenue.

Un cas pratique permettra de mieux cerner le problème, celui du filtrage évolué du protocole '**SNMP**' dont les données sont structurées en **ASN.1** au format **BER** et généralement en forme concise étant donnée la faible taille des structures. Certains filtres vont alors directement rechercher le code correspondant à la requête - '**get**', '**getnext**' ou '**set**' par exemple - à une position fixe et ceci pour des raisons d'efficacité.

Cette méthode fonctionne parfaitement dans le cas des implémentations standards. Cependant rien n'interdit de transmettre une requête identique mais encodée dans une forme alternative telle que la position à laquelle est recherchée l'identification de la requête contienne une valeur autorisée par la règle de filtrage.

On notera à ce propos qu'il y a quelques années, l'implémentation du protocole '**snmp**' dans les systèmes Windows posait problème à certains équipements de filtrage, **Microsoft** ayant choisi d'encoder l'une des structures de données dans sa forme 'longue' décalant ainsi d'un octet la position du code de la requête.

Nous concluons en rappelant que comme toujours dans le domaine de la sécurité, l'essentiel n'est pas d'assurer une sécurité absolue mais d'être informé et de connaître les limitations des technologies et de leur implémentation afin d'y palier par la mise en place des procédures ad'hoc.

Dans l'exemple cité précédemment, le plus grand risque n'était pas celui généré par la limitation fonctionnelle du produit, connue de l'éditeur mais non documentée, mais la méconnaissance de celle-ci qui laissait croire à l'utilisateur qu'il était totalement protégé. La simple documentation du problème aurait permis à ce dernier de choisir librement d'utiliser ou non cette fonctionnalité en connaissance de cause.

• Complément d'information

<http://www.uniras.gov.uk/vuls/2003/006489/x400.htm>
<http://www.uniras.gov.uk/vuls/2003/006489/smime.htm>
<http://www.uniras.gov.uk/vuls/2003/006489/openssl2.htm>
<http://www.niscc.gov.uk/News/newsnov03.pdf>
<http://luca.ntop.org/Teaching/Appunti/asn1.html>
<http://www.isi.salford.ac.uk/books/osi/chap8.html>
<http://asn1.elibel.tm.fr/oid/>
http://www.itu.int/itu-t/rec/x/x200-499/x208_22887.html
http://www.itu.int/itu-t/rec/x/x200-499/x209_24177.html

- Alerte X400
 - Alerte SMIME
 - Alerte OpenSSL
 - Article d'accompagnement
 - Le guide ASN.1
 - Un excellent historique
 - ASN.1 OID
 - Norme X208 (DER)
 - Norme X209 (BER)